Simplifying Cyber Security since 2016

HACKERCOOL

September 2025 Edition 8 Issue 9

Red Teaming against AI-Powered Defenses: Tactics, Techniques and Tools for 2026

in

RED TEAM HACKING

VULNERABILITY FOR BEGINNERS

Inside CVE-2025-20333: The zero-day flaw in Cisco ASA firewalls that is already under active exploitation

BLUE TEAM HACKING

Open-source tools every Blue Team should know

VULNERABILITY FOR BEGINNERS

How are threat actors logging in into SonicWall's SSLVPN devices without brute-forcing?

MOBILE SECURITY

Inside Klopatra: The stealthy Android Trojan draining bank accounts and taking complete control of the device

Copyright © 2025 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publishe -r, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed “Attention: Permissions Coordinator,” at the address below.

Any references to historical events, real people, or real places are used fictitiously. Na -mes, characters, and places are products of the author’s imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com

HACKERCOOL

Simplifying Cybersecurity

DISCLAIMER

Information provided in this Magazine is strictly for educational purpose only. Please don't misuse this knowledge to hack into devices or networks without taking relevant permissions. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 8 Issue 9

Welcome to this month's issue of Hackercool Magazine, where we dive headfirst into the evolving—and often unsettling—landscape of digital defense and offense. As we step closer to 2026, the line between attacker and defender continues to blur, powered by advancements in AI, automation, and adaptive threat strategies.

In this issue, we start with a look inside the future of Red teaming against AI-powered defenses, unpacking the next generation of tactics, techniques, and tools security professionals must master. The battlefield is changing, and human creativity remains the ultimate exploit.

Our vulnerability coverage this month is extensive and essential. From the Chrome zero-day (CVE-2025-10585) already under active exploitation, to critical exposures in Gladinet's Triofox (CVE-2025-11371) and Cisco ASA firewalls (CVE-2025-20333), we break down what these flaws mean for your environment—and how to respond before attackers do.

For defenders, we feature a deep dive into open source tools every Blue Teamer should know about in our article "Open-source tools every Blue Team should know".

On the privacy front, our "Anonymous Zone" explores Tails 7.0, the latest release of the go-to OS for anonymity, while our "Mobile Security" section exposes the stealth and sophistication behind "Klopatra", an Android trojan designed to drain bank accounts and hijack entire devices.

We also review the latest updates in recently released Kali Linux 2025.3, keeping penetration testers and researchers informed of the newest features and tools that keep the community sharp.

As always, cybersecurity is not just about tools—it's about awareness, adaptability, and constant learning. Whether you're red, blue, or somewhere in between, this issue aims to keep you ahead of the next exploit.

Stay vigilant,
Kalyan Chinta,
Editor-in-Chief, Hackercool Magazine

Contact us:

Mail: admin@hackercoolmagazine.com

WhatsApp/Telegram: +919505658443

INSIDE

See what our Hackercool Magazine's September 2025 Issue has in store for you.

1. Red Team Hacking:
Red Teaming against AI-Powered Defenses: Tactics, Techniques and Tools for 2026

2. Vulnerability for beginners:
CVE-2025-10585: Zero-day vulnerability in Chrome already under active exploitati -on

3. Blue Team Hacking:
Open-source tools every Blue Team should know about.

4. Vulnerability for beginners:
CVE-2025-11371: LFI zero-day in Gladinet Triofox

5. What's New:
Kali Linux 2025.3

6. Vulnerability for beginners:
CVE-2025-20333: The zero-day in Cisco ASA firewalls already under active exploitation.

7. Anonymous Zone:
Tails 7.0 is released: What's New

8. Vulnerability for beginners:
How are threat actors logging in into SonicWall SSLVPN devices without brute-forcing?

9. Mobile Security:
Inside Klopatra: The stealthy Android trojan draining bank accounts and taking complete control of the phone

10. Cybersecurity:
The world's most sensitive computer code is vulnerable to attack. A new encryptio- n method can help.

Red Team Hacking
Red Teaming against AI-Powered Defenses

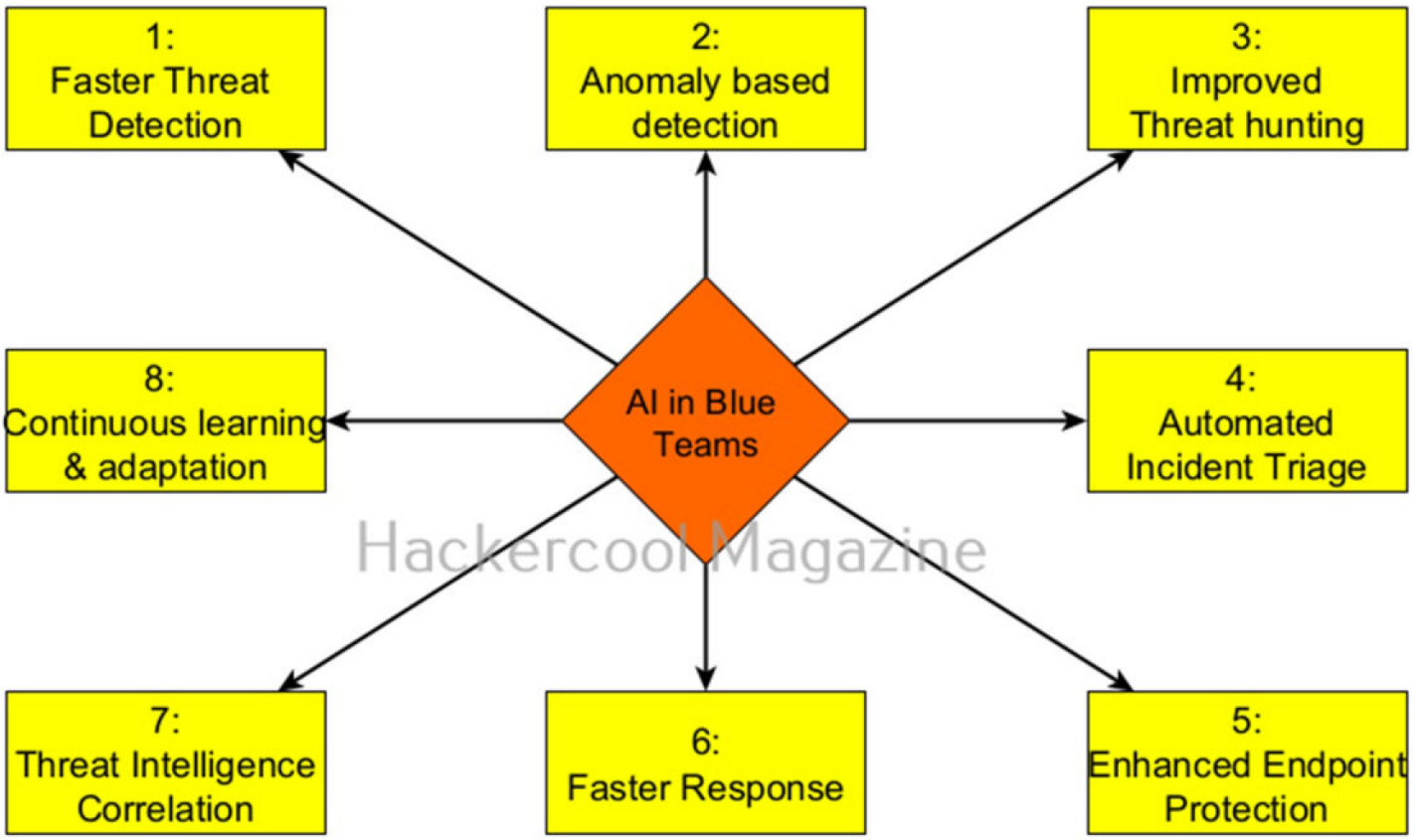
Like everything, Artificial Intelligence (AI) is changing cyber battlefield too very fast. It is being used by both attackers and defenders to good use. While attackers are using AI to make their attacking techniques more sophisticated, Blue teams are using AI to improve their defense techniques. This employm-ent of AI by Blue teams poses a never before challenge to Red Teams durin-g engagement. In the feature of this month's Issue, we bring our readers ho-w Red Teams should fight against AI-powered Defenses in 2025.

Why Blue teams are opting for AI powered defenses

The Rise of AI in Blue teaming provides a lot of advantages to the blue tea-m. Most important of them are given below.

> AI red teaming is emerging as one of the most effective first steps businesses can take to ensure safe and secure systems today. But security teams can't approach testing AI the same way they do software or applications. You need to understand AI to test it."
> – Chris Thompson, Global Head, IBM X-Force Red

Fig: Advantages of AI for Blue Teams



1. Faster Threat Detection

AI models can analyze huge volumes of logs, events and telemetry data in r-eal time, identifying malicious behavior patterns faster than traditional rule-based systems and humans.

For example, AI can detect unusual login times or impossible travel anom-alies across systems. Let's say a user logs in from New Delhi and then logs i-n from Tokyo 10 minutes later. This reduces mean time to detect (MTTD), catching attackers early in the kill chain.

2. Anomaly & Behavior-based detection

AI powered defenses can perform behavioral analytics, detecting unknown threats based on deviations from normal behavior. On the contrary, traditio-

nal defenses can only detect malicious behaviour using known signatures (e.g., specific malware hashes).

For example, User and Entity Behavior Analytics (UEBA) models can flag a user downloading 10GB of data from a file server when they usually acces -s only a few MB. This catches zero-day attacks and insider threats that bypa- ss signature-based systems.

3. Improved Threat Hunting

AI assists threat hunters by identifying and classifying suspicious events, clu -stering related incidents and highlighting patterns across vast datasets. For e- xample, AI can correlate process creation, registry modification and related network activity to suggest a potential PowerShell-based attack. This reduces time to find advanced threats and supports proactive defense.

4. Automated Incident Triage

AI helps prioritize alerts by context and severity filtering out false positives and escalating only meaningful threats. For example, AI can rank alerts bas- ed on historical threat patterns, criticality of the asset under target and poten- tial impact. This cuts down alert fatigue and lets analysts focus on real issues.

5. Enhanced Endpoint Protection

AI-powered EDR/XDR platforms analyze low-level system activity (e.g., pr- ocess behavior, memory usage, system calls) and flag or block suspicious be- havior before it escalates. For example, AI can detect fileless malware by ob -serving abnormal PowerShell behavior. This ability prevents attacks that by- pass traditional antivirus solutions.

6. Faster Response & Containment (SOAR Integration)

AI, when integrated with Security Orchestration, Automation, and Respon-

se (SOAR) enables automated playbooks for containment and remediation. This can allow AI to identify a malware outbreak and automatically isolate a -ffected machines, reset credentials and notify admins. This speeds up mean time to respond (MTTR), thus limiting damage.

7. Threat Intelligence Correlation

AI can cross-reference telemetry with real-time threat intel feeds, identifyin-g known actor TTPs, indicators of compromise (IOCs) or attack campaigns. For example, AI can easily flag activity similar to an APT known to target y-our sector, like credential stuffing from IPs tied to recent breaches. This feat-ure can improve contextual awareness and strategic defense.

8. Continuous Learning & Adaptation

Modern AI models can learn from new attacks, adapting detection mecha-nisms without needing manual rule updates. This keeps defenses evolving al -ongside threats, which is very crucial as attacker tactics shift constantly.

Common AI Defense Mechanisms to Challenge

Fig: Common AI Defense Mechanisms

Organizations use various AI defense mechanisms to protect from hacking

attacks. Prominent among them are,

1. AI-Driven Intrusion Detection & Prevention (IDPS)

Intrusion detection and prevention engines are increasingly relying on deep learning to identify zero-day attacks, traffic patterns and user behavior anomalies.

Red Team Focus: The focus of Red teams while dealing with AI-driven IDPS should be to simulate adversaries who adapt to AI-driven security systems and use adversarial machine learning to bypass them.

2. Automated Threat Hunting Tools

Machine Learning (ML) algorithms that predict threats based on historical data—are increasingly becoming part of SIEM (Security Information and Event Management) tools, such as Splunk or Elastic SIEM.

The focus of the Red Teams while dealing with these should be to figure out how to evade detection by generating minimal or false positive anomalies.

3. Automated Incident Response

Many blue teams now deploy automated playbooks (e.g., SOAR platforms) that take immediate action on detected threats, isolating networks, blocking IPs or changing configurations.

The focus of the Red teams in this case should be to simulate attacks that not only evade detection but can also cause these automated systems to malfunction or escalate incorrectly.

Red Team Strategies for Evasion and Exploitation

Red Teams can use various techniques to evade and exploit AI-powered d

efences. They are,

1. Adversarial Machine Learning for Evasion:

For all their positive qualities, AI systems are only as strong as the data they're trained on. Adversarial Machine Learning (model poisoning) can manipulate AI decisions, tricking AI defenses into misidentifying threats.

Red Teams should focus on techniques for introducing subtle inputs to confuse or deceive AI algorithms. For example, using adversarial noise to bypass anomaly detection.

2. AI and Deepfake-based Social Engineering

Deepfakes (video/audio) and synthetic media are now widely used in social engineering attacks, creating convincing impersonations of key individuals (executives, technical staff, etc.).

Red Teams should leverage AI to craft realistic deepfake content for phishing, impersonation, or vishing (voice phishing)..

3. Evading ML-Based Behavioral Analysis

Many AI defenses use behavioral baselining to differentiate deviations from normal user activity. Red Teams can employ strategies like mimicking typical user behaviors or gradually escalating suspicious activity to avoid detection.

This can be done using slow, steady escalation tactics, implementing living-off-the-land techniques using native tools and scripts to avoid raising flags.

Key Tools and Techniques for Red Teams

Done well, red teaming can identify and help address vulnerabilities in AI. What it does not do is address the structural gap in regulating the technology in the public interest."
-Brian Chen, Director of Policy, Data & Society

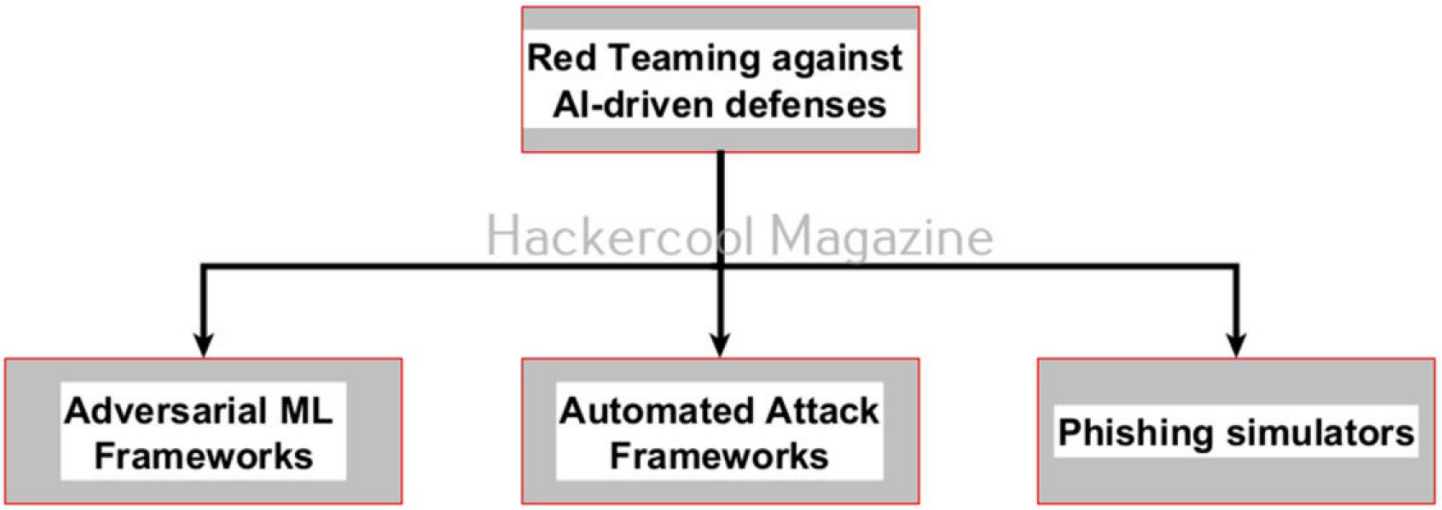


Fig: Key techniques of Red Teams against AI-driven defenses

Red Teams can use many tools in their quest to defeat AI powered defences. Some of them are,

1. Adversarial ML Frameworks

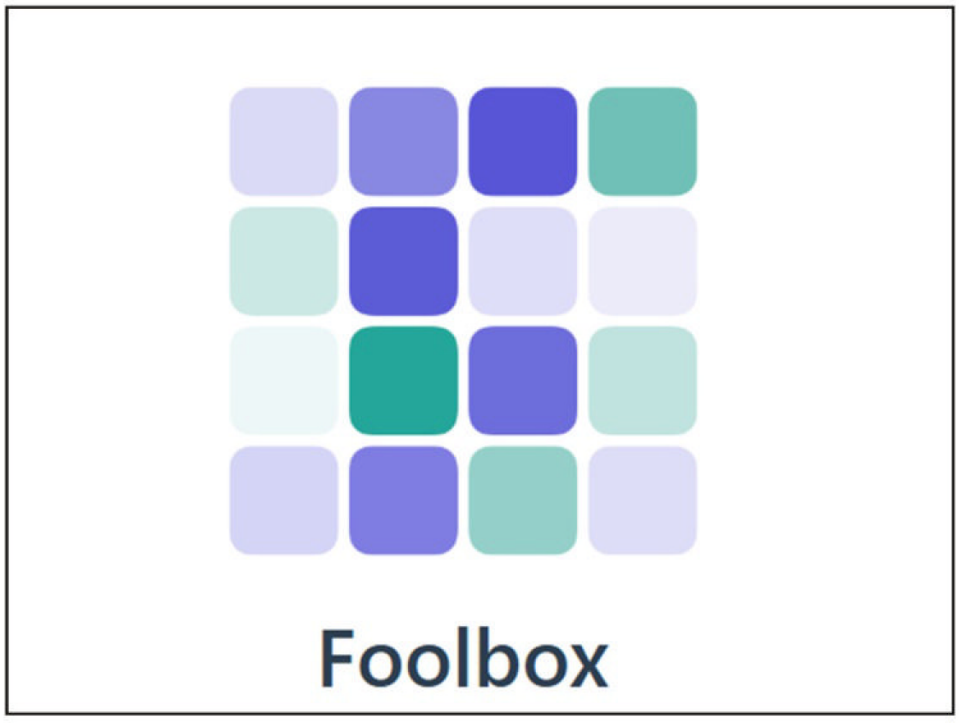
An adversarial ML framework in red teaming refers to the systematic application of adversarial machine learning (AML) techniques to identify and exploit vulnerabilities within AI systems, particularly machine learning models, during a red team exercise. This framework aims to simulate real-world attacks to assess the robustness, security and resilience of AI-powered defenses. Some of the tools in this category are,

CleverHans: CleverHans is an open-source, Python library designed to create adversarial examples to attack ML models.

"AI is in the hands of the bad guys. And the reality is that they use it more and more. ... We need to redesign the systems. We need to make them not just secure, we need to make them immune."

–Eugene Kaspersky, Founder, Kaspersky Lab

Foolbox: It is a Python toolbox to create adversarial examples that fool neural networks in PyTorch, TensorFlow and JAXTool.



ART (Adversarial Robustness Toolbox): An open-source Python toolbox that can create adversarial examples for testing ML model security.

2. Automated Attack Frameworks for AI/Evasion Tactics

Tools in this category include,

Metasploit: Continues to evolve to integrate AI-driven exploits. Red teams can use Metasploit's capabilities to emulate adversaries leveraging AI-powered evasion techniques.

Empire (PowerShell-based post-exploitation framework): Integrates tactics f-
or AI evasion and persistence strategies.

```
==========================================================
 [Empire]  Post-Exploitation Framework
==========================================================
 [Version] 2.0 | [Web] https://theempire.io
==========================================================

      267 modules currently loaded

      0 listeners currently active

      0 agents currently active

(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > info
[!] Invalid listener name
```

3. Phishing Simulators & Synthetic Media Tools

DeepFaceLab (deepfake tool): To create realistic face swaps for imperso-
nation.

Resemble.AI: Can generate synthetic voices for social engineering or impersonation in vishing attacks.

Steps for Red Teams testing AI-Driven Defenses

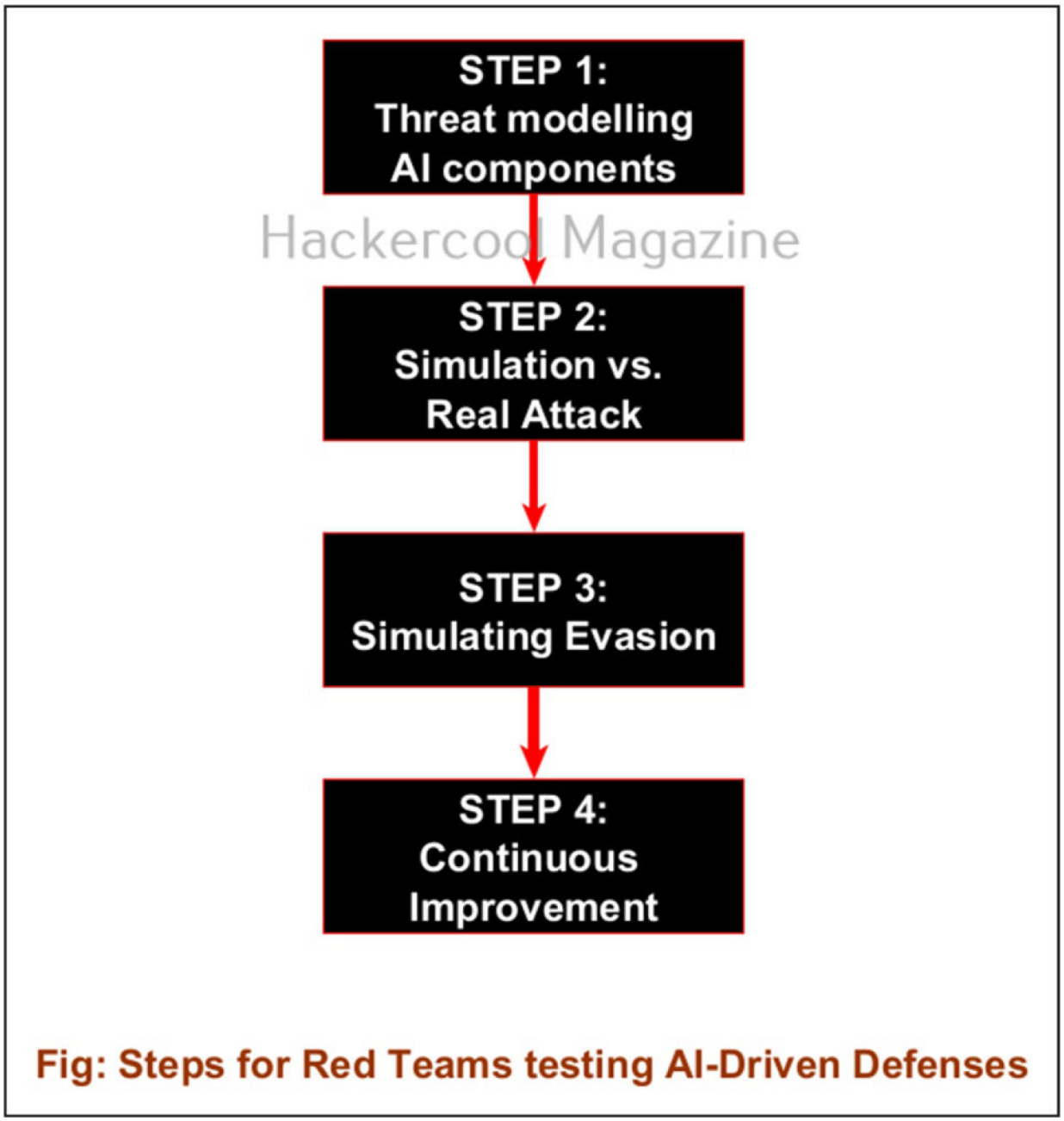


Fig: Steps for Red Teams testing AI-Driven Defenses

Step 1: Threat Modeling AI Components
First, understand how AI systems in use are trained, tested and operational-ized. Focus on their training data, decision processes, and where adversarial manipulation might be possible.

Step 2: Simulation vs. Real Attack
Use purple team tactics (cooperative exercises) to safely assess AI defense's strength and weaknesses. This helps both red and blue teams learn the most effective attack vectors while refining response strategies.

Step 3: Simulating Evasion
Red teams can simulate the effects of adversarial examples or introduce minor behavioral changes that make AI defenses misinterpret or overlook attacks. Tricks like modifying traffic patterns or credentials in such a way that a traditional IDS system would miss.

Step 4: Continuous Improvement
As AI tools evolve rapidly, red teamers must also continually update their playbooks. Automate and scale attack simulations to test evolving AI defenses. For example, build an automated pipeline that continuously tests how AI tools respond to new exploits and TTPs.

Key Considerations

1. Legal & Ethical Boundaries while testing AI

Engaging in adversarial testing or creating deepfakes can raise ethical concerns, especially when simulated attacks involve impersonation of real individuals. Always ensure consent, particularly when dealing with PII or potentially defamatory content.

2. Disclosure & Remediation

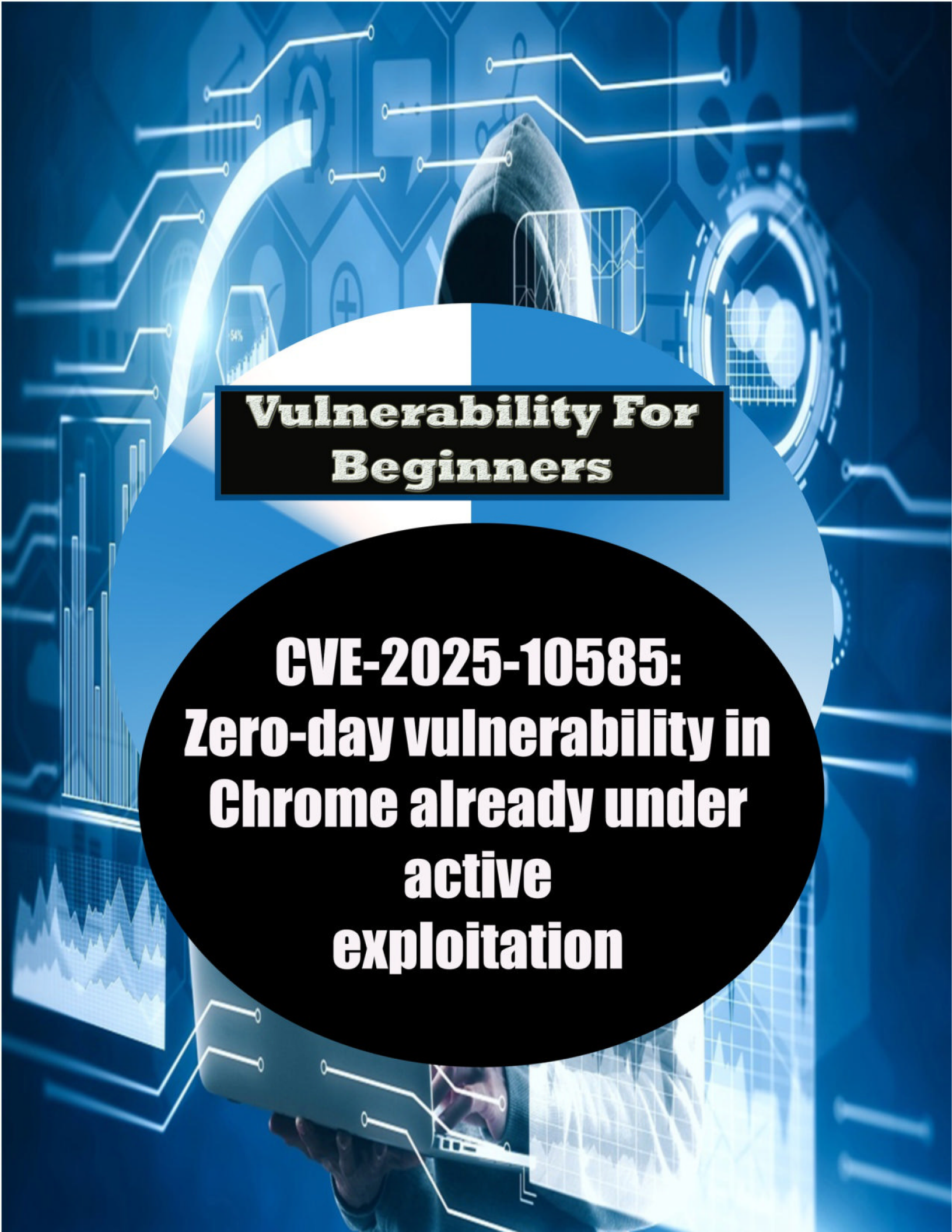
When red teaming against AI systems, it's essential to work with blue teams in a responsible manner. This involves clear reporting structures and remedi

-ation strategies for AI weaknesses discovered during the engagement.

Conclusion

As AI becomes more integrated into both offense and defense, red teams will need to continuously evolve their tactics. Staying ahead means understa-ding the technologies behind the defenses and anticipating how adversaries will use AI for attack automation. Not just that, Red teams must collaborate closely with blue teams to provide feedback on AI defense effectiveness. Tr-aining on AI threat vectors will be crucial for upskilling both offensive and d-efensive teams.

This part of the page has been intentionally left blank


Vulnerability For Beginners
CVE-2025-10585: Zero-day vulnerability in Chrome already under active exploitation

Google Chrome has released an urgent security update to fix four vulnerabilities including a critical vulnerability that is being actively exploited in real-world.

Hackercool Magazine

CVE-2025-10585: Zero-day vulnerability in Chrome already under active exploitation

About the vulnerabilities

The four vulnerabilities that have been fixed in Chrome are CVE-2025-10585, CVE-2025-11458, CVE-2025-11460 and CVE-2025-11211. Dangerous among them is CVE-2025-10585 which is a zero-day vulnerability that is already being exploited in real-world by threat actors. It is a critical Type Confusion vulnerability in the V8 JavaScript and WebAssembly feature of Chromium engine with a CVSS v3.1 base score of 9.8. Type confusion vulnerabilities are considered very dangerous as they can be weaponized by threat actors to trigger unexpected software behaviour which includes execution of malicious code.

CVE-2025-10585 is the sixth zero-day vulnerability detected in Chrome browser that has been either actively exploited or demonstrated as a proof-of-concept (PoC) this year. The five zero-days in Chromium prior to this are CVE-2025-2783, CVE-2025-4664, CVE-2025-5419, CVE-2025-6554 and CVE-2025-6558. All of them have been discussed in our previous Issues.

The versions of Chrome browser vulnerable to this vulnerability are all versions prior to 140.0.7339.185 for Windows and Apple macOS and versions prior to 140.0.7339.185 for Linux.

How hackers can exploit CVE-2025-10585?

Hackers can exploit this vulnerability remotely by creating a maliciously cr-afted HTML page and luring target users to that page.

Impact

Google Chrome is used by millions of users around the world. CVE-2025-10585 can result in heap corruption, memory corruption and subsequently malicious code execution remotely. The vulnerability affects Chromium V8 engine which is not just used by Google Chrome browser but also other chromium-based browsers like Microsoft Edge, Opera, Vivaldi and Brave. T-his makes this vulnerability especially critical.

CISA has added this vulnerability to its Known Exploited Vulnerabilities (KEV) catalog on September 23, 2025 confirming that threat actors are lever-aging it in real-world attacks. It is not yet known which threat actor is exploi-ting it but the involvement of Google's TAG in the vulnerability's discovery points to a state-sponsored threat actor.

How to manage this vulnerability?

Since Google has already released patches for this vulnerability and others and this vulnerability being exploited in real-world, users should update thei-r browsers as soon as possible. The versions of Chrome browser that fixes t-his vulnerability are 140.0.7339.185/.186 for Windows and Apple macOS an-d 140.0.7339.185 for Linux. You can update your Chrome browser to the lat-est version by going to **Chrome menu>Help or Settings> About chrome**. This will install any pending updates automatically. Immediate patching is advised.

People using other popular browsers that are Chromium-based – like Edg-e, Brave, Opera and Vivaldi should look out for patches from the respective developers and apply them ASAP.

BLUE TEAM HACKING

OPEN-SOURCE TOOLS EVERY BLUE TEAM SHOULD KNOW

Blue teams, whether in a small security operation center (SOC) of a small startup or a large enterprise face the same problem. They have more things to protect in an organization than budget or people to watch them. That's w-here the role of open-source tools becomes important for every blue team.

Why open source matters for Blue Teams

Open source software (OSS) is crucial for blue teams because it offers a cost-effective access to powerful security tools without the licensing fees of co-mmercial alternatives. The auditability of open-source tools allows defenders to inspect code for backdoors, vulnerabilities or compliance with internal sta-ndards which are very critical in high-trust environments. Open source Blue team tools also enable deep customization, letting teams tailor tools to their u-nique threat models and infrastructure.

The open-source community around these tools often drives rapid innovati-on and knowledge sharing, helping defenders keep pace with evolving thre-

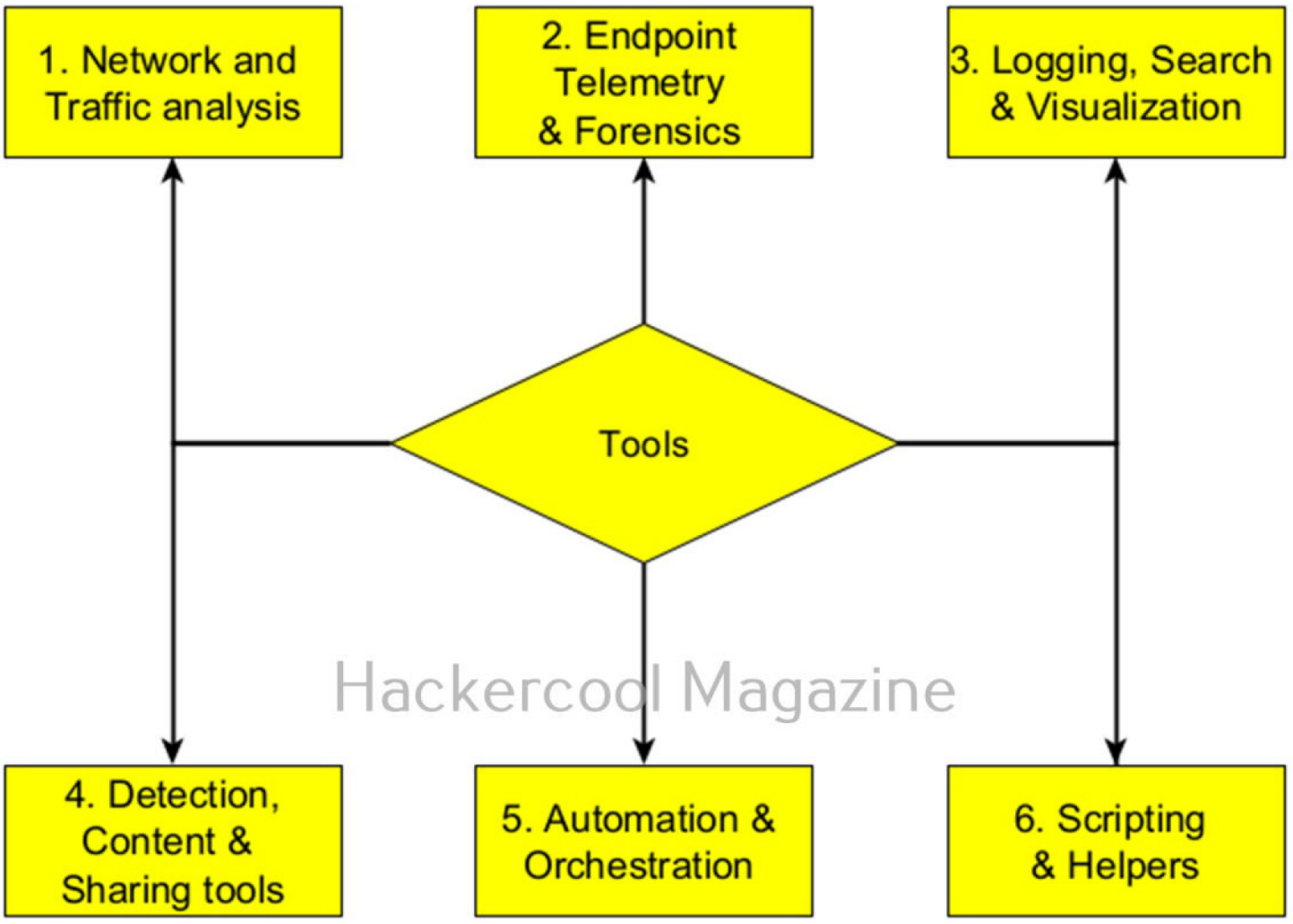
ats. Additionally, open source projects can be adopted and deployed quick-ly, giving teams an edge when time matters.

In this month's "Blue Team Hacking" feature, we bring you a list of popula-r open-source tools that play an important role in Blue teaming around the world.

How to read this list?

We have divided this list of open-source tools into different categories for e-asier understanding.

Fig: Classification of open-source Blue Team Tools

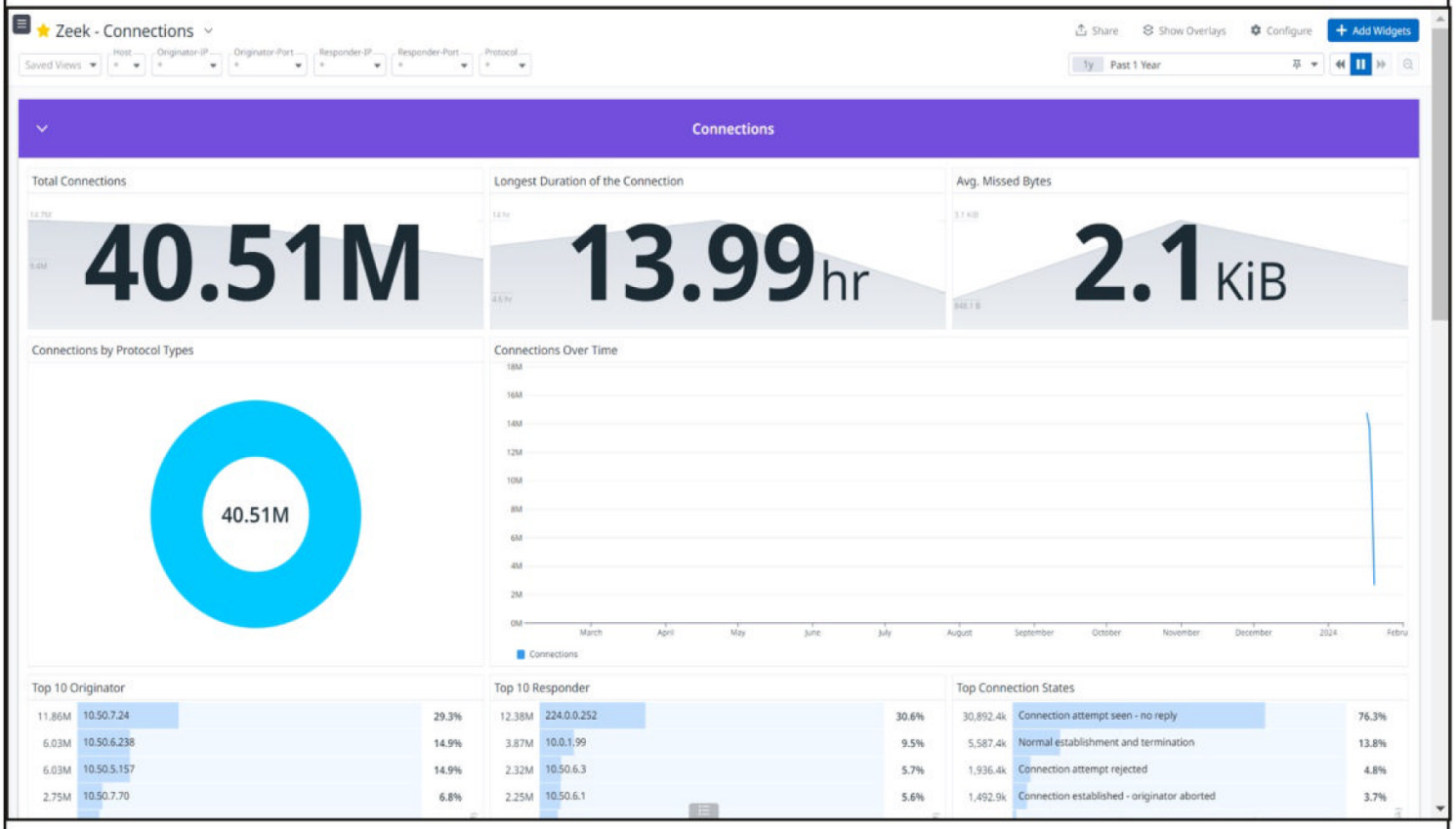


The categories are Network & Traffic analysis, Endpoint, Logging/Analytics, Incident Response/Forensics, Threat Intelligence, Rule/Detection Formats an-d Automation. Note: each entry gives a 1-line description, primary use case, and a 2–3 command quick-start.

1. Network and Traffic analysis:

This enables Blue teams to rapidly detect network-based intrusion, C2, later-al movement, exfiltration and reconnaissance, separate noisy benign traffic fr-om suspicious/hostile patterns. Here are some open-source tools that help yo-u in network and traffic analysis.

Zeek: Zeek is a network security monitor (NSM) that can also be used as a network intrusion detection system (NIDS). It allows you to perform protocol-aware passive network analysis that is excellent for extracting logs a-nd building detection rules.



Suricata: Suricata is an open-source Intrusion Detection System (IDS) and I-ntrusion Prevention System (IPS). It provides threat detection capabilities an-d traffic filtering and monitoring capabilities. It can help in detecting comm-

-on attack vectors such as port scanning, denial-of-service, pass-the-hash attac-ks and even brute-force attacks.

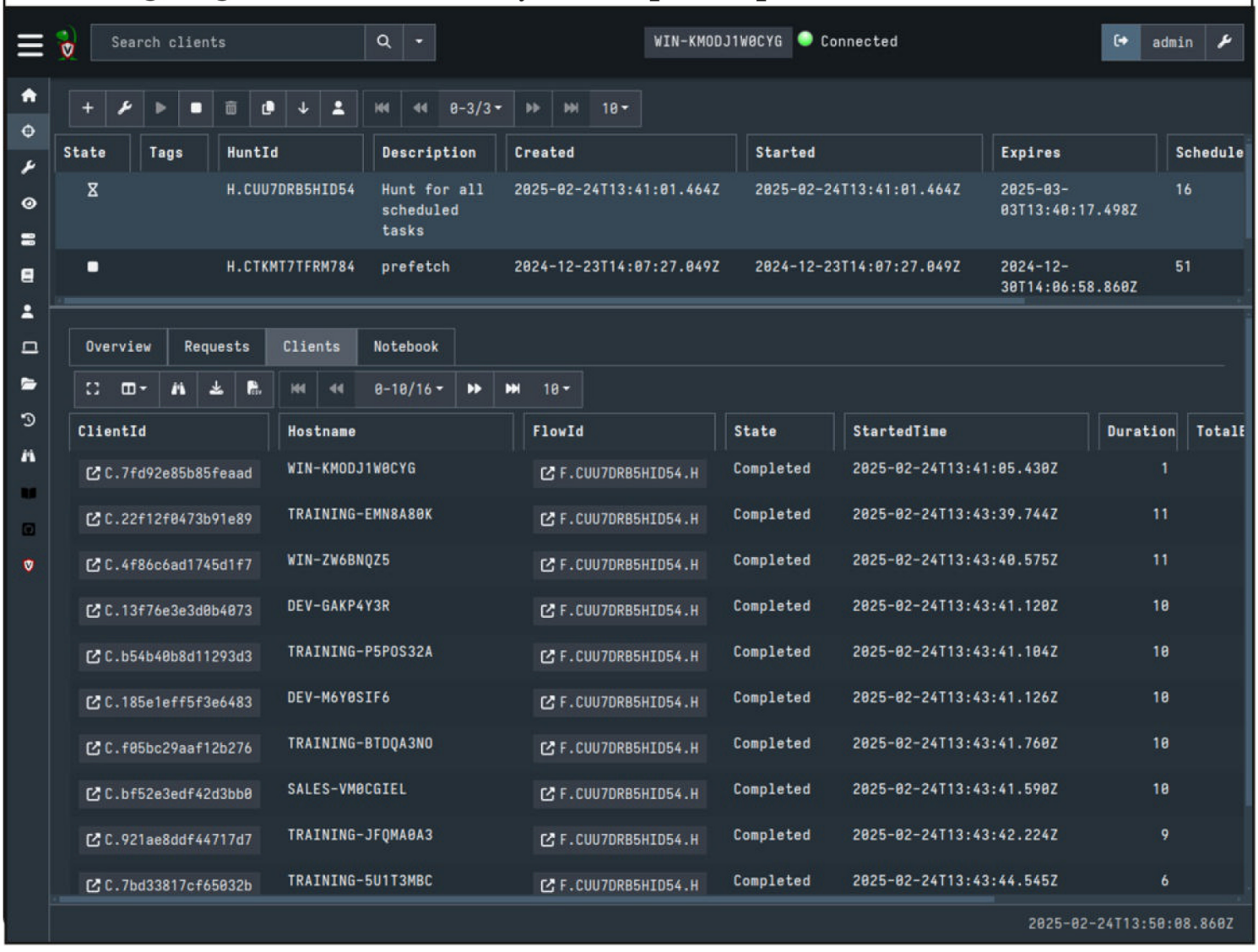
2. Endpoint Telemetry & Forensics

It detects malicious activity like credential theft and lateral movement early and preserves forensic evidence in a forensically-sound way. Here are the to-ols to help you in this.

Osquery: Osquery is an open-source tool that exposes an operating syste-m's status as a relational database, allowing users to query it using SQL-like commands. It acts as an operating system instrumentation framework for pla

> "Cybersecurity is much more than just a technical problem. It's also a psychological and organizational one." – Bruce Schneier

Velociraptor: Velociraptor is a unique, advanced open-source endpoint m -onitoring, digital forensic and cyber response platform.



Fleet (or Kolide): Fleet is an open-source platform that helps security professionals manage, secure, and monitor a large number of devices, such as laptops and servers. It is built on the OSquery tool, which allows blue teams to treat their infrastructure like a database and run SQL-like queries to gather information and detect threats.

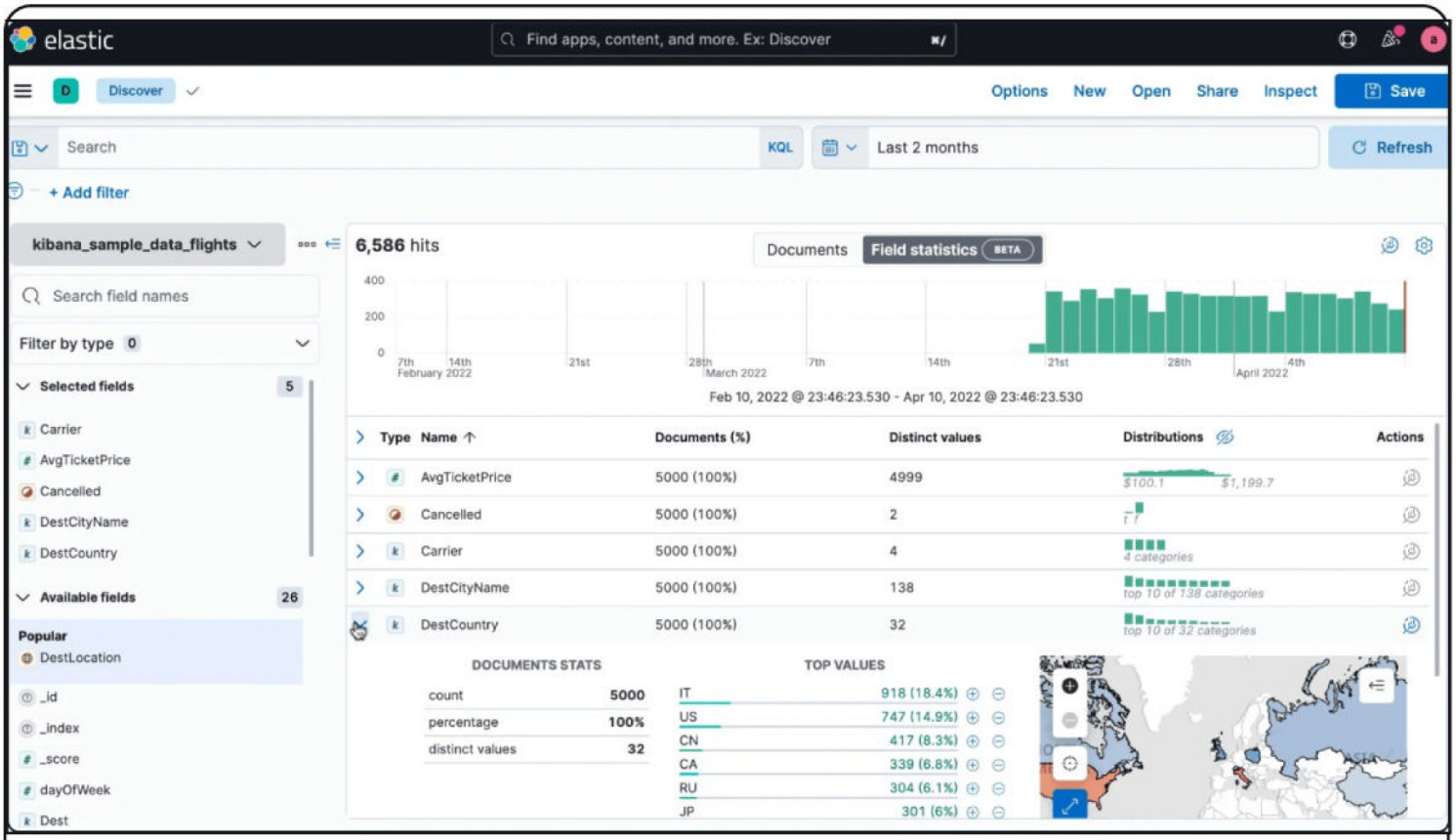
3. Logging, Search & Visualization

In Blue teaming, centralized ingestion is very important as it allows defenders to have a unified view of activity across the entire environment. Centralized ingestion means collecting and consolidating data (logs, telemetry, alerts, metrics, etc.) from multiple sources — such as endpoints, servers, network devices, cloud platforms, and applications — into a single, centralized location or platform for analysis, correlation, and monitoring.

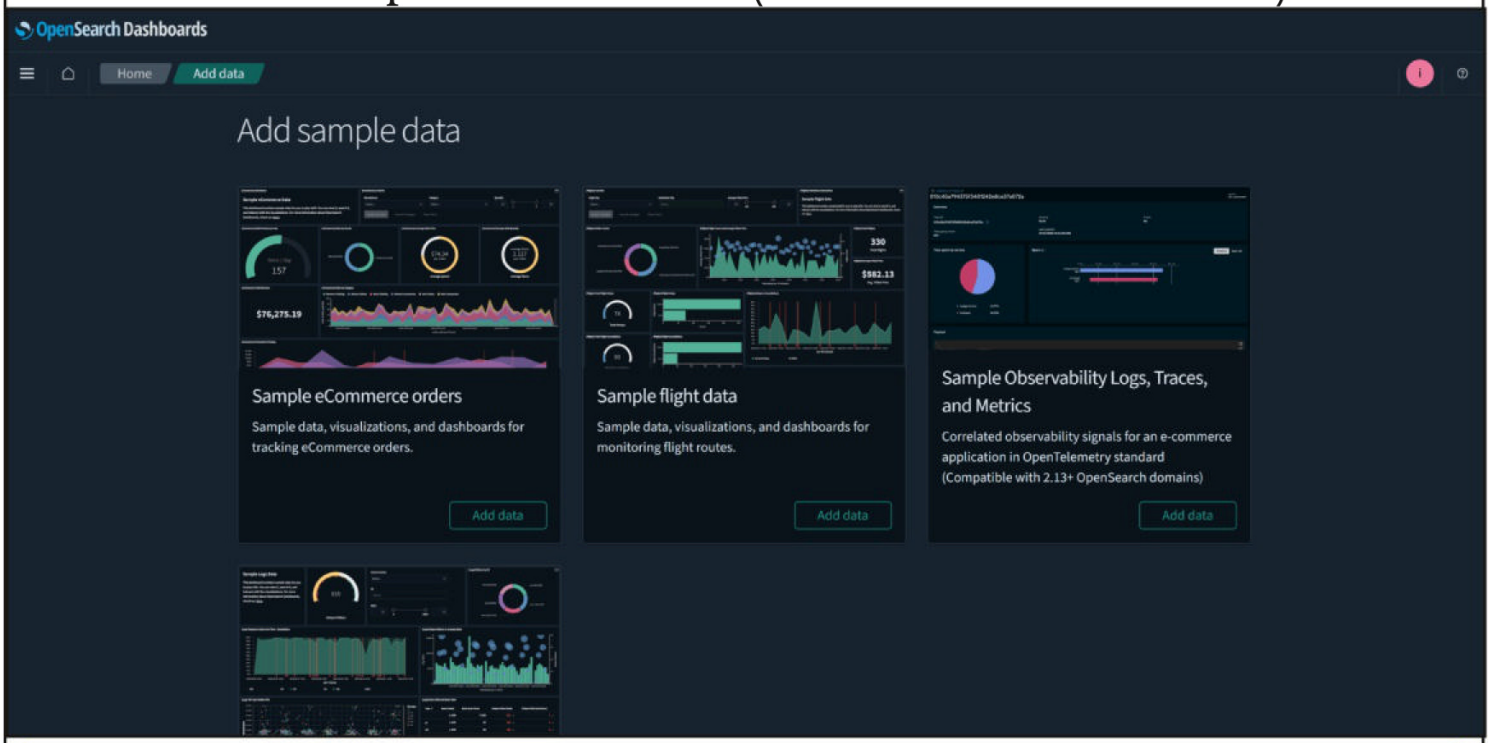
Any Logging tool should have schema and retention. Schema is the structured format that defines how data fields are named, typed, and organized when ingested and retention is how long you store telemetry and logs before they're deleted, archived, or rolled off your SIEM or data lake.

Schema is important in blue teaming as any logging tool should have consistent detection logic, easier correlation, efficient hunting, portability and maintaining data quality. Retention is important in blue teaming for incident response and forensics, For example, hacking attacks often go unnoticed for weeks or months. You need historical data to reconstruct the timeline. (E.g., you detect a backdoor today that was dropped 90 days ago.). Retention is also useful in threat hunting, detection tuning, Compliance, Baselining & anomaly detection and Root cause analysis. Some of the best open source tools Blue teams could use for logging are,

ElasticSearch: Elasticsearch is a powerful search and analytics engine used to store, search, and analyze security logs and data to monitor, detect, and respond to threats. It's part of the Elastic Stack (ELK Stack) that contains Elasticsearch + Logstash + Kibana (+ Beats).



OpenSearch: OpenSearch is a fully open-source fork of Elasticsearch and Kibana, created by Amazon (AWS) in 2021 after Elastic changed Elasticsear -ch's license from Apache 2.0 to SSPL (Server Side Public License).



"Open-source continuous security testing is not a luxury — it is integral to sustaining a SOC's effectiveness." -David Hunt, CTO, Prelude

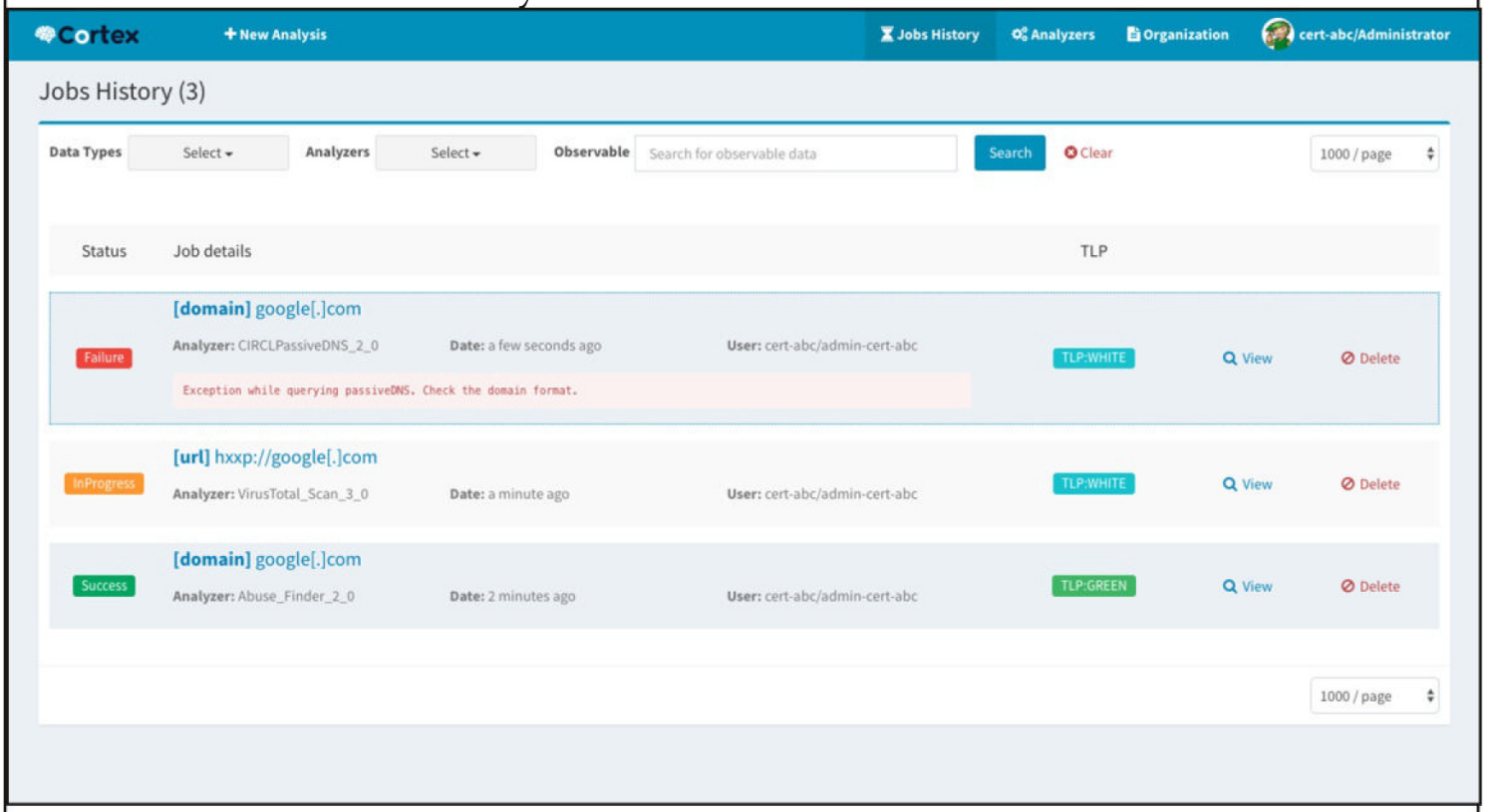
4. Detection Content & Sharing tools

Sigma: Sigma is an open, vendor-agnostic rule format for describing detect -ion logic (searches/alerts) in a structured, human-readable YAML format.

YARA: YARA is a lightweight, flexible pattern-matching language and too -l used to identify and classify malware, suspicious files, and in-memory artifacts by describing their textual/binary characteristics as rules.

MISP: Shortcut for Malware Information Sharing Platform & Threat Sharing, MISP is an open-source threat intelligence platform (TIP) designed to create, store, share, correlate and operationalize cyber threat intelligence (indicators, TTPs, sightings, reports) across teams and trusted communities.

TheHive + Cortex: TheHive and Cortex are two tightly integrated, open-source tools that are useful in case management and automated analysis. They're designed to help SOCs and CSIRTs in triaging alerts, investigate incidents and run automated enrichment and response actions for case management and automated analyzers.

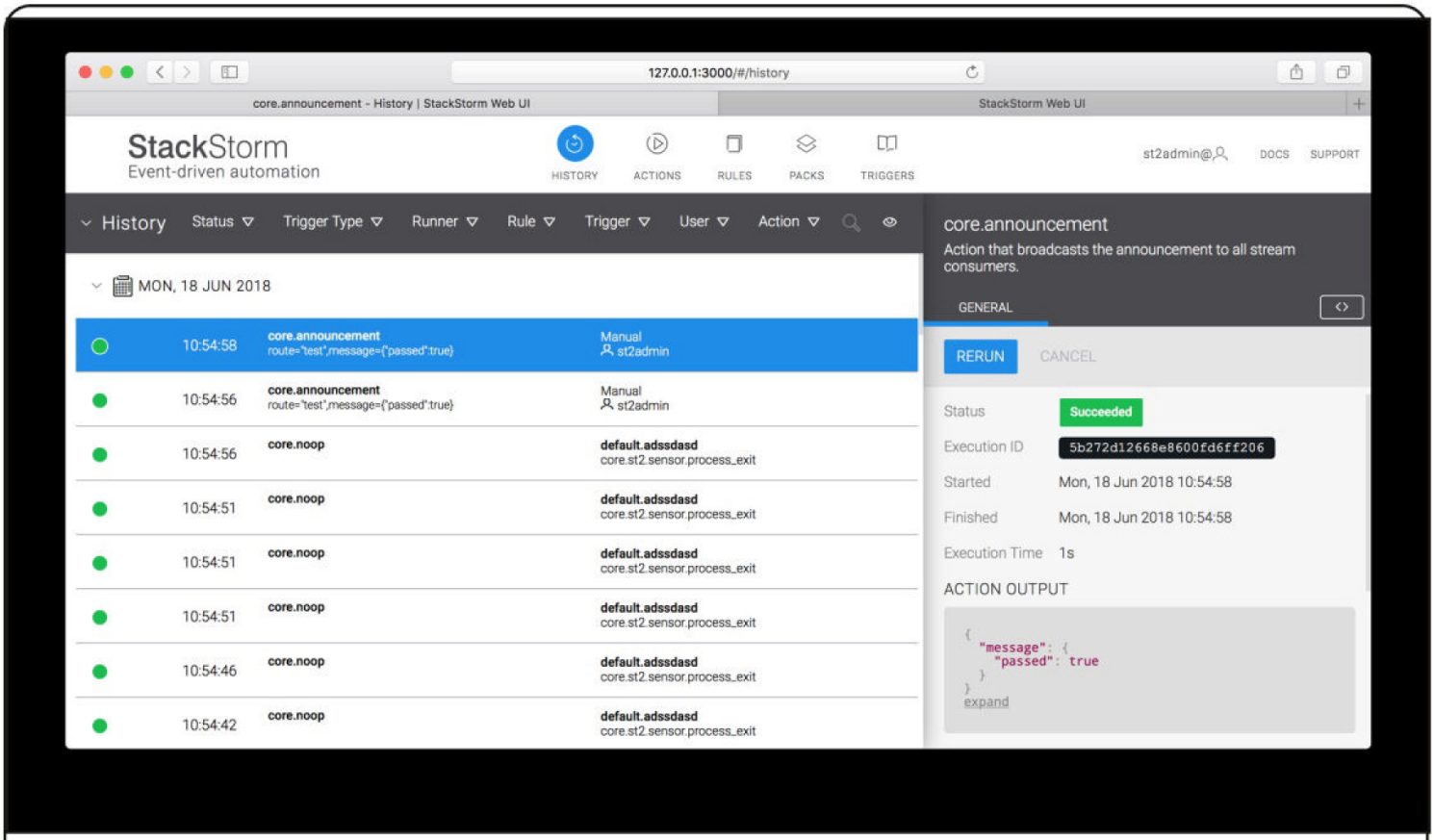


Automation & Orchestration

Automation and Orchestration help in speeding up blue team operations, maintain consistency, manage large scale alert volumes, collect evidence & auditability etc. Tools in this category are clubbed under SOAR which stands for Security Orchestration, Automation, and Response.

SOAR options: StackStorm, Shuffle, Cortex (analysers), and playbooks with TheHive integrations. Emphasize small automation wins.

"Something is inherently different about open source that makes it more viable for security analysis. ... Open source gives you the total flexibility needed to build a rich cybersecurity SOC platform. ... Besides, you can't afford to 'test' the non-free stuff."
–Joe Gresham, Senior Developer, onShore Security.



6. Scripting & Helpers

Scripting + helper tools are the everyday toolkit that let you automate triage, collect evidence, enrich IOCs, hunt across logs, and glue systems together. Tools her are gawk, jq, pcap tools, Netcat etc

Open-source tools aren't a panacea, but when stitched together thoughtfully they give blue teams transparency, control and an extraordinary amount of capability for the cost of time. Start small, automate predictable work and make sure every tool you deploy answers the question: "How does this help us detect, triage, or respond?" If it can't, don't install it — just refine or repurpose it.

"At a micro level, the blue team consists of the individuals directly responsible for monitoring, defending, and responding to incidents. At a macro level, the blue team is the entire organization, including the end users and customers."–Marcus J. Carey, Cybersecurity community advocate

Vulnerability For Beginners
CVE-2025-11371:
LFI Zero- day in Gladinet Triofox

Cybersecurity company Huntress has detected a zero-day vulnerability under active exploitation in real-world affecting Gladinet Centrestack and Trio-Fox products. Gladinet Centrestack and TrioFox are enterprise file-sharing and cloud storage solution that provide secure VPN less remote access to files.

About the vulnerabilities

The zero-day vulnerability being tracked as CVE-2025-11371 with a CVSS score of 6.1 is an unauthorized local file inclusion vulnerability that allows unauthorized users to view system files. All versions of Gladinet Centrestack and Triofox prior to 16.7.10368.56.560 are vulnerable.

"We are one year away from AI conducting real attacks autonomously."
-Kevin Mandia, Founder of Mandiant

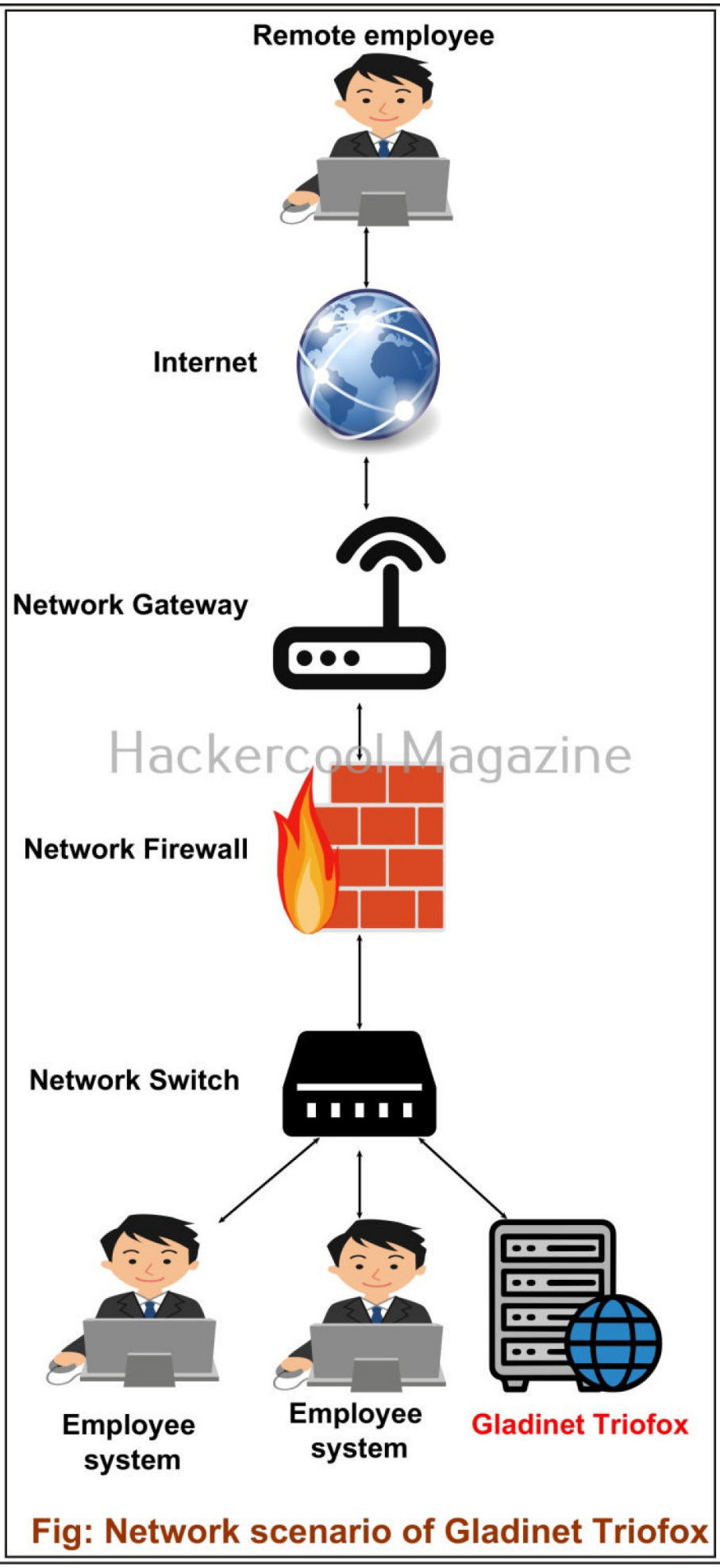


Fig: Network scenario of Gladinet Triofox

Earlier, both Gladinet centrestack and Triofox were affected by CVE-2025-30406 (with a CVSS score of 9.0) that allowed hackers to perform remote co-de execution by exploiting a view state deserialization vulnerability that allo-wed them to retrieve a hard-coded machine key.

The present vulnerability also allows hackers to retrieve the machine key fr-om the application web.config file to perform RCE attack using the same vi-ew state deserialization vulnerability we explained above. In the present cas-e however, Huntress found hackers exploiting version 16.4.10315.56368, a v-ersion not vulnerable to CVE-2025-30406, which suggests hackers are exploi-ting the latest vulnerability to retrieve the hardcoded machine key and use it to perform RCE through view state deserialization flaw.

How this vulnerability can be exploited?

To exploit this vulnerability, hackers are sending an unusual “GET reques-t” to “/storage/t.dn” endpoint. This request prompted the server to show a co-py of the web.config file.

Usually the requests to this endpoint is handled by “Gladinet Storage.Temp. Download” function that has been programmed to retrieve fi-les from the “temp” directory for authenticated users.

Impact

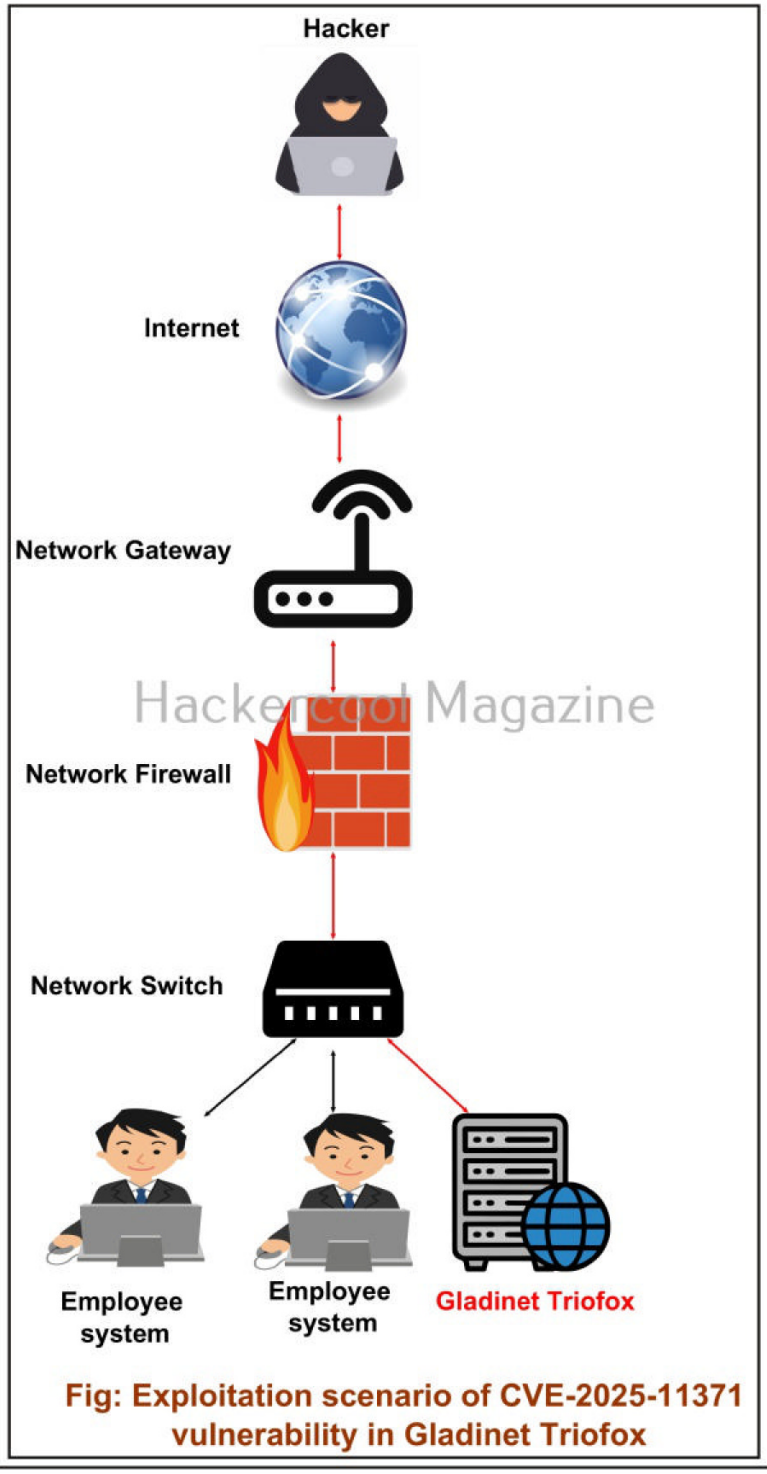
As already mentioned above, the vulnerability is already being exploited in real-world. The exact number of users for Gladinet CentreStack and TrioFox is available but Huntress estimates there are a few hundred vulnerable serve-rs exposed to internet. Hackers can exploit this vulnerability access any file o-n the remote target system without authentication.

How to manage this vulnerability?

On Oct 4, 2025, Gladinet released version 16.10.10408.56683 of Centrestac

-k and Triofox that includes a fix for CVE-2025-11371. Users are advised to apply the latest fix as soon as possible.

If applying fixes is not possible, users should disable the “temp” handle wit-hin the web.config file located at C:\Program files\ Gladinet cloud Enterpris-e\uploadDownload Proxy\web.config. This may affect some of the tool’s fun-ctionality but it will make sure that this vulnerability cannot be exploited. R-emoving the TEMP handle removes access to the “t.dn” endpoint. After dis-abling the handle, restart the web service to make sure changes take effect.



Hackercool Magazine

Fig: Exploitation scenario of CVE-2025-11371 vulnerability in Gladinet Triofox

What's New
Kali Linux 2025.3

The third release of Kali this year, Kali 2025.3 has been released recently.

Let's see what's new in the latest release. To those who have no idea, Kali Linux is a penetration testing, Red teaming distro.

Latest features to be excited about

New tools

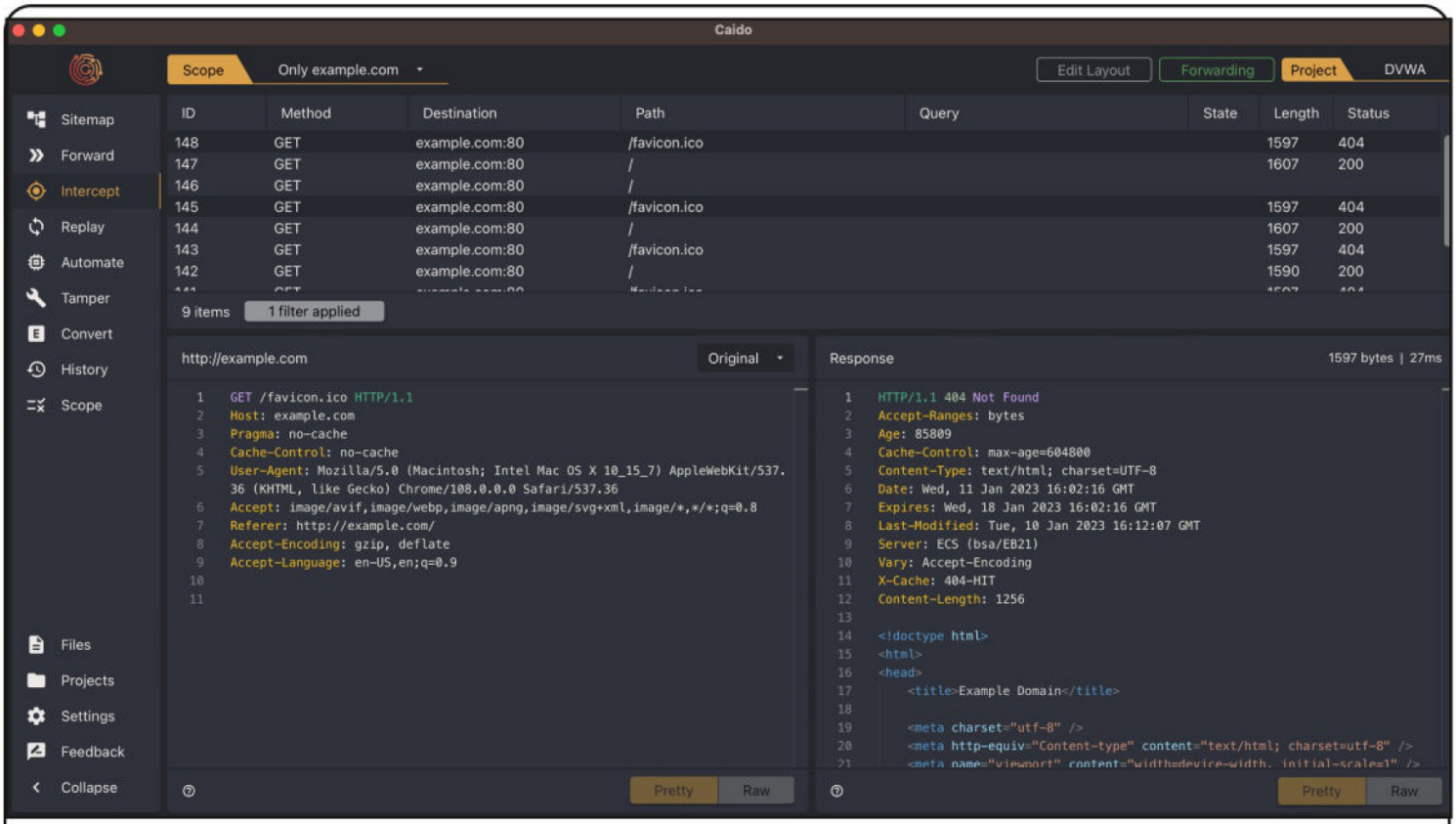
What is a new release of Kali if it doesn't have new tools? This release adds 10 new tools to its network repositories. Important among them are,

1) Caido and Caido-cli

The client side and server side of Caido a web security auditing toolkit has been added.

"Corporate security is not about attack and defense. The term blue team connotes a game or a match, one side against the other ... but most of the time you're having a discussion with a colleague about finding the best way to build something or make it better."

-Wendy Nather, Director, Advisory CISOs at Duo Security



2) Vwifi-dkms: Helpful tool to set "dummy" wi-fi networks.

3) Detect It Easy (DIE): A powerful tool for file type identification used widely by malware analysts, cyber security experts and reverse engineers.

```
┌──(kali㉿kali)-[~]
└─$ diec
Usage: diec [options] target
Detect It Easy v3.10
Copyright(C) 2006-2008 Hellsp@wn 2012-2024 hors<
horsicq@gmail.com> Web: http://ntinfo.biz


Options:
  -h, --help                    Displays help on
commandline options.
  --help-all                    Displays help inc
luding Qt specific options.
  -v, --version                 Displays version
information.
```

Hackercool Magazine

4) Gemini CLI: An open-source AI agent that brings the power of Gemini directly into terminal.

```
┌──(kali㉿kali)-[~] Hackercool Magazine
└─$ gemini-cli
```

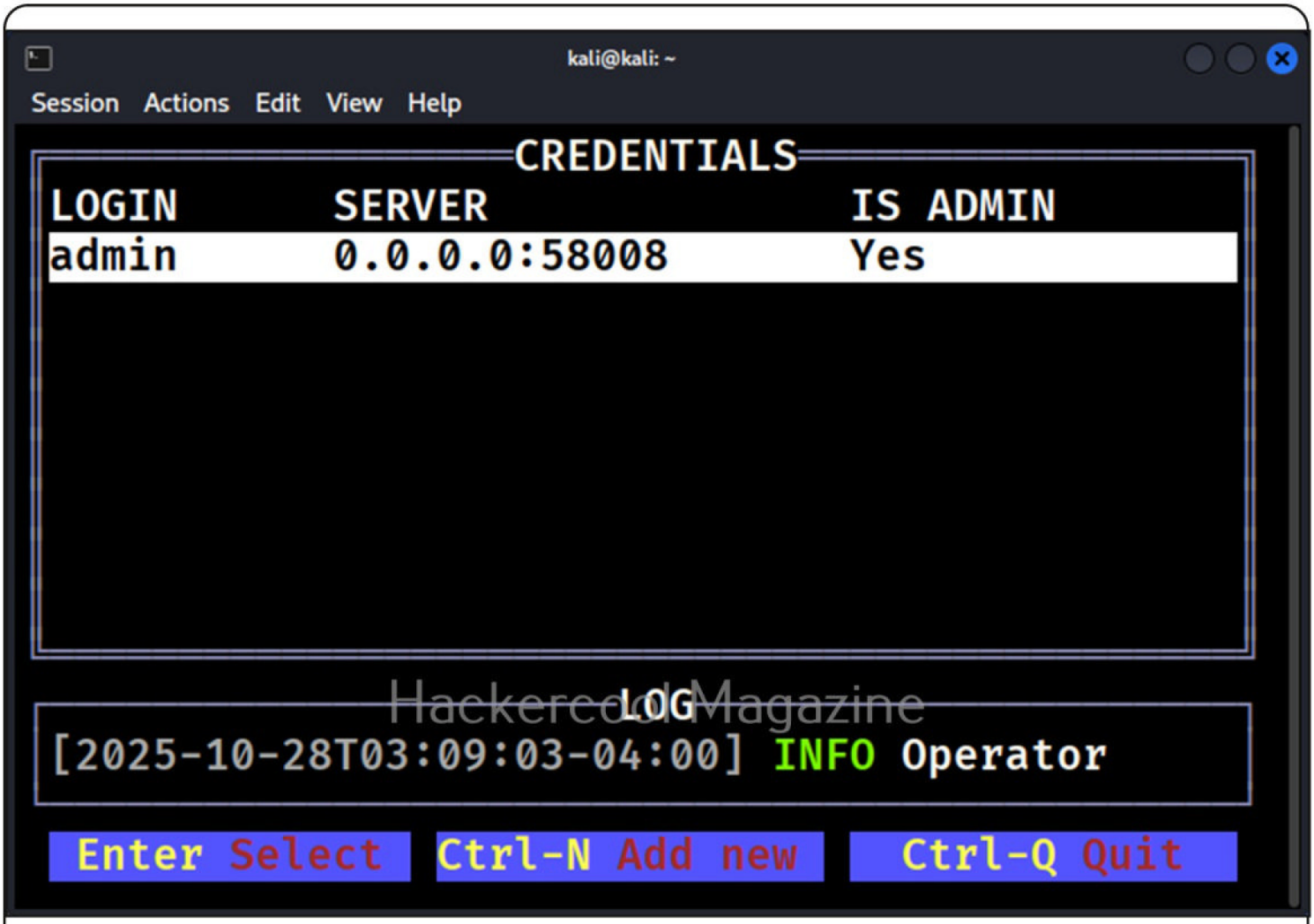
5) Krbrelayx: Kerberos relaying and unconstrained delegation abuse toolkit.

```
┌──(kali㉿kali)-[~]
└─$ krbrelayx
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Running in export mode (all tickets will be
saved to disk). Works with unconstrained delegat
ion attack only.
[*] Running in kerberos relay mode because no cr
edentials were specified.
[-] You need to specify at least one relay targe
t, or specify credentials to run in unconstraine
d delegation mode
```

Hackercool Magazine

6) Ligolo-mp: An advanced version of Ligolo-ng. A client server model th-at enables penetration testers to play with multiple concurrent tunnels.

"The attack surface is changing, and the rise of machine identities is at the core of it. Securing these identities is just as critical as protecting human ones if businesses want to stay secure."
–Phil Calvin, Chief Product Officer at Delinea



7) LLM-tools-nmap: A plugin for LLM's tool that provides Nmap network scanning capabilities. This plugin enables LLM's to perform network discovery and security scanning tasks using the powerful Nmap tool.

8) Mcp-kali-server: This app allows the MCP to run terminal commands like nmap, nxc etc.

"What are your contingency plans? Because attacks will get through. Have you got them on paper somewhere in case all your systems really go down?"

—Anne Keast-Butler, Head of GCHQ

```
┌──(kali㉿kali)-[~]
└─$ kali-server-mcp
2025-10-28 03:13:59,393 [INFO] Starting Kali Lin
ux Tools API Server on port 5000
 * Serving Flask app 'kali_server'
 * Debug mode: off
2025-10-28 03:13:59,431 [INFO] WARNING: This is
a development server. Do not use it in a product
ion deployment. Use a production WSGI server ins
tead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://192.168.249.145:5000
2025-10-28 03:13:59,431 [INFO] Press CTRL+C to q
uit
```

9) Patchleaks: A tool that supports security fixes by comparing two versio-ns of code base

```
┌──(kali㉿kali)-[~]
└─$ patchleaks
[2025-10-28 03:14:44,404] INFO in app: PatchLeak
s startup

╔═══════════════════════════════════════════════
═══════════════════╗
║                          PatchLeaks Started
                   ║
╚═══════════════════════════════════════════════
═══════════════════╝
  Server URL: http://127.0.0.1:2005
```

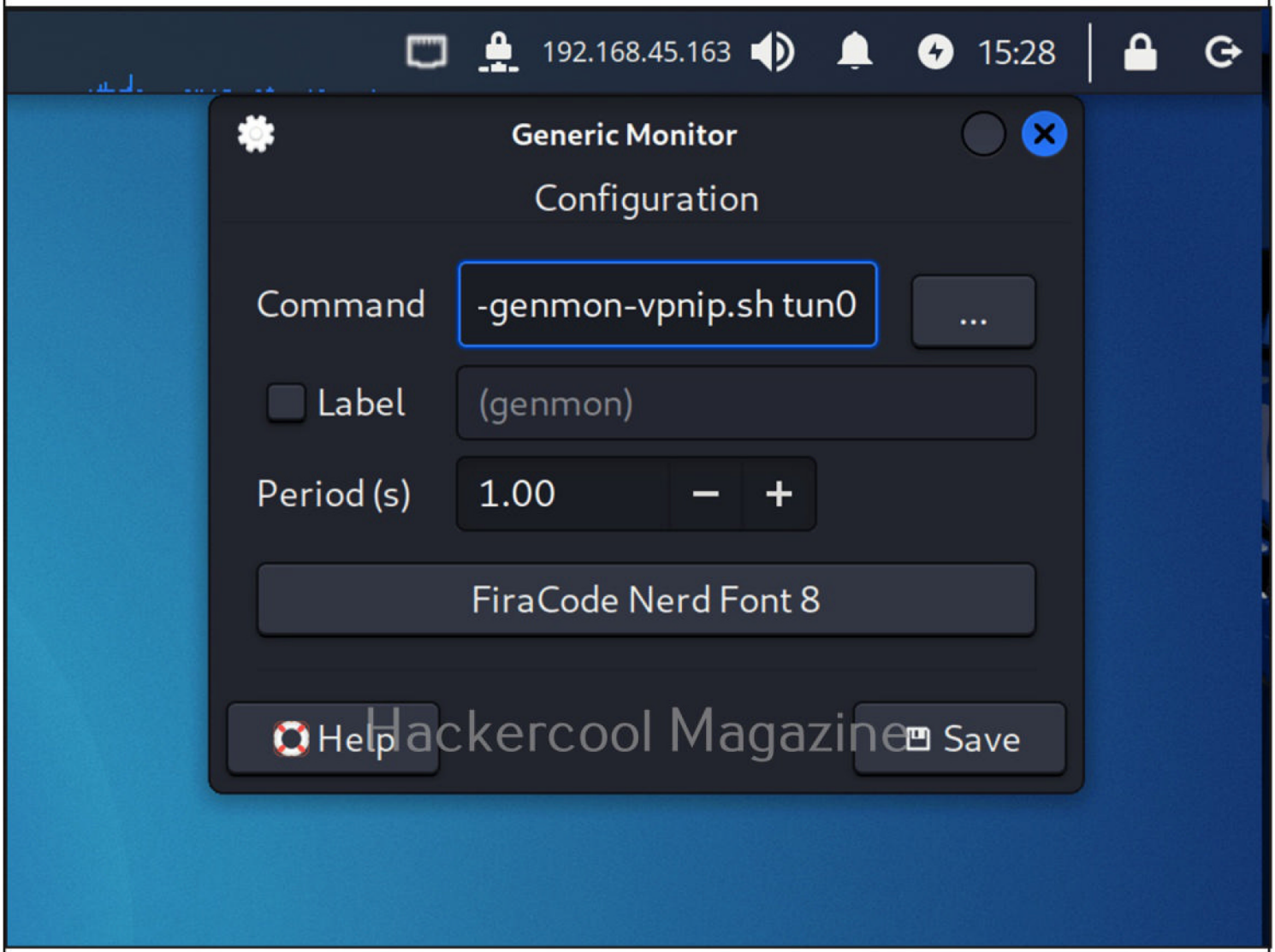
```
╔═══════════════════════════════════════════════════════════════════════
═══════════╗
║  ⚠  IMPORTANT: Save these credentials!                               
           ║
║  They are randomly generated each time the app starts.               
           ║
╚═══════════════════════════════════════════════════════════════════════
═══════════╝

 * Serving Flask app 'app'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:42005
Press CTRL+C to quit
```

Hackercool Magazine

Other important updates added

VPN IP panel plugin



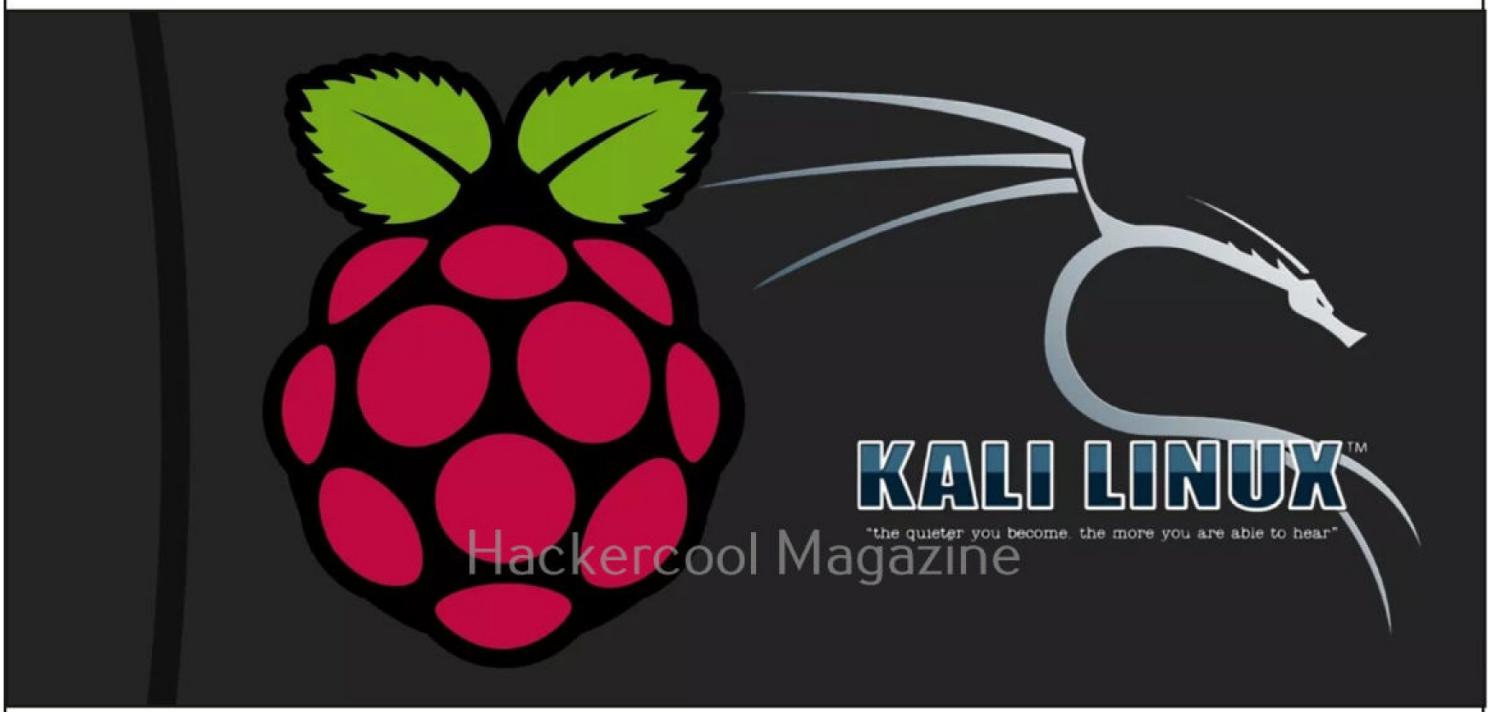
The VPN IP panel plugin that was introduced in kali 2024.1 got an upgrade. Earlier it was only possible to view the IP of the first VPN. This release adds an option to choose from multiple VPN IPs.

2) NetHunter updates

Kali NetHunter too got many updates. Kali Net Hunter now supports Samsung Galaxy S10. The NetHunter'a car hacking app, CARsenal also got lot of features added and hence expanded. To apply the new changes however,

you need to run the setup again.

3) Kali ARM updates



This release adds Nexmon support to ARM devices. Nexmon is a “patched” firmware for certain wireless chips. It extends functionality to mo -nitoring and injection mode capabilities.

The wireless chips that support Nexmon are Broadcom and Cypress. Apart from Nexmon, ARM kali has been improved.

Other updates added

Dropped support to ARMel

With this release, Kali has dropped support for ARMel (Acorin RISC Mac -hine, little-Exdian). That’s because Debian Trixie 13 (the latest stable versio-n) is the last release with ARMel support. Debian testing which Kali is based on, doesn’t provide support to ARMel packages.

Conclusion

These are all the new features added to the latest release of Kali. Which on -e among these is your favorite.

“They appear to have valid credentials. The speed at which they are directly logging into multiple accounts without any brute forcing attempts prior shows that they have either valid credentials or that they have figured out another way to log in.”

—Jamie Levy, Director of Adversary Tactics at Huntress, commenting on SSLVPN devices compromised on SonicWall.

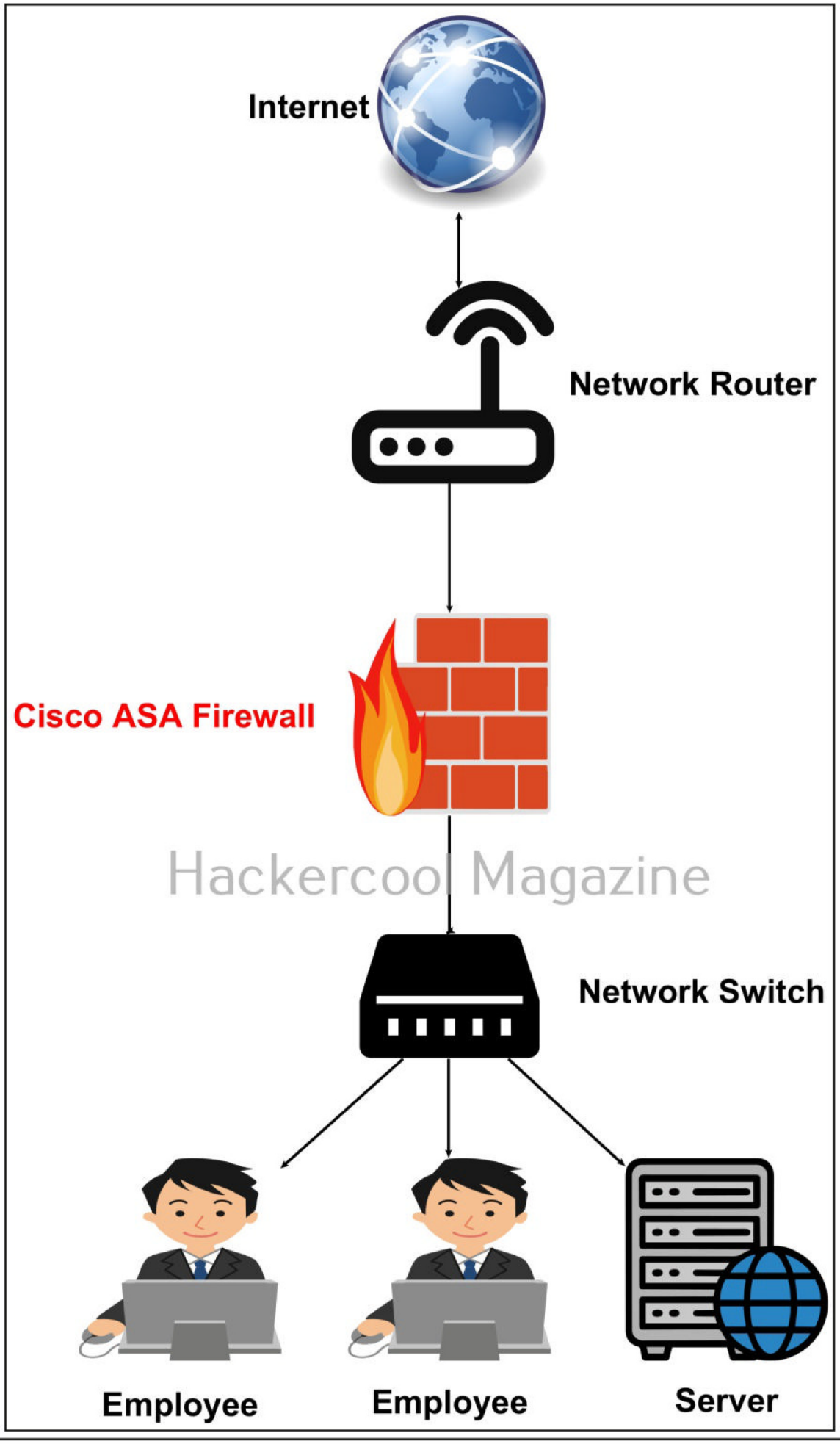
Vulnerability For Beginners
CVE-2025-20333: The zero-day in Cisco ASA firewalls under active exploitation

A critical zero-day vulnerability affects thousands of Cisco ASA firewalls is being actively exploited by threat actors in real-world.

About the vulnerabilities

The vulnerability being tracked as CVE-2025-20333 has a CVSS score of 9.9. The vulnerability affects Cisco Secure Firewalls Adaptive Security Appli-ance (ASA) and Cisco Secure Firewalls Threat Defense (FTD) software. Th-e affected versions are Cisco ASA 9.12, 9.14, 9.16 to 9.20 and 9.22 to 9.23 a-nd FTD versions 7.0 to 7.4 and 7.6 to 7.7.

It specially affects the VPN web server components. The vulnerability is an improper validation of user-supplied input in HTTP (s) requests processed b-y the VPN web server. It allows authenticated remote attackers to trigger a buffer overflow and execute malicious code with root privileges on vulnera-ble devices.


Internet
Network Router
Cisco ASA Firewall
Hackercool Magazine
Network Switch
Employee
Employee
Server

Devices running vulnerable release of ASA or FTD software with specific configuration enabled are affected by this vulnerability. These configurations are critical enterprise features the organization use for secure remote access. They are Any Connect, IKEV2, Remote Access, Mobile User Security (M-US) and SSL VPN services.

Another vulnerability CVE-2025-20362 that was also under exploitation by unauthenticated attackers to access restricted VPN endpoints that is actually only accessible using authentication. It can serve as a reconnaissance tool for hackers to plan advanced attacks.

How hackers exploit this vulnerability?

To exploit this vulnerability, hackers need valid VPN credentials to login. Once they successfully authenticate, they can send malicious HTTP requests containing malicious payloads to overflow buffer. They can then execute shellcode with the privileges of root user.

Although requirement of credentials can limit its exploitation, hackers can easily obtain them using methods like credentials stuffing, spear phishing or exploiting weak passwords.

Impact

Once exploited, it can give hackers complete control of the Cisco ASA firewall. This enables attackers to modify security policies, monitor network traffic and install backdoors. Seeing that the vulnerability is already being exploited in real-world, it can be estimated that hackers already have correct credentials. Millions of users use Cisco VPN services so impact of the vulnerability can be gauged. It is estimated that nearly 50,000 Cisco ASA and FTD firewalls are vulnerable and majority of these (19,000) are located in USA.

CISA said that these threat actors are successfully exploiting this vulnerability are the same threat actors who previously targeted the same Cisco products in 2024. This time however, they are deploying new malware named RayInitiator, Viper etc. It is being suspected that both these vulnerabilities

CVE-2025-20333 and CVE-2025-20362 are being chained to bypass authentication.

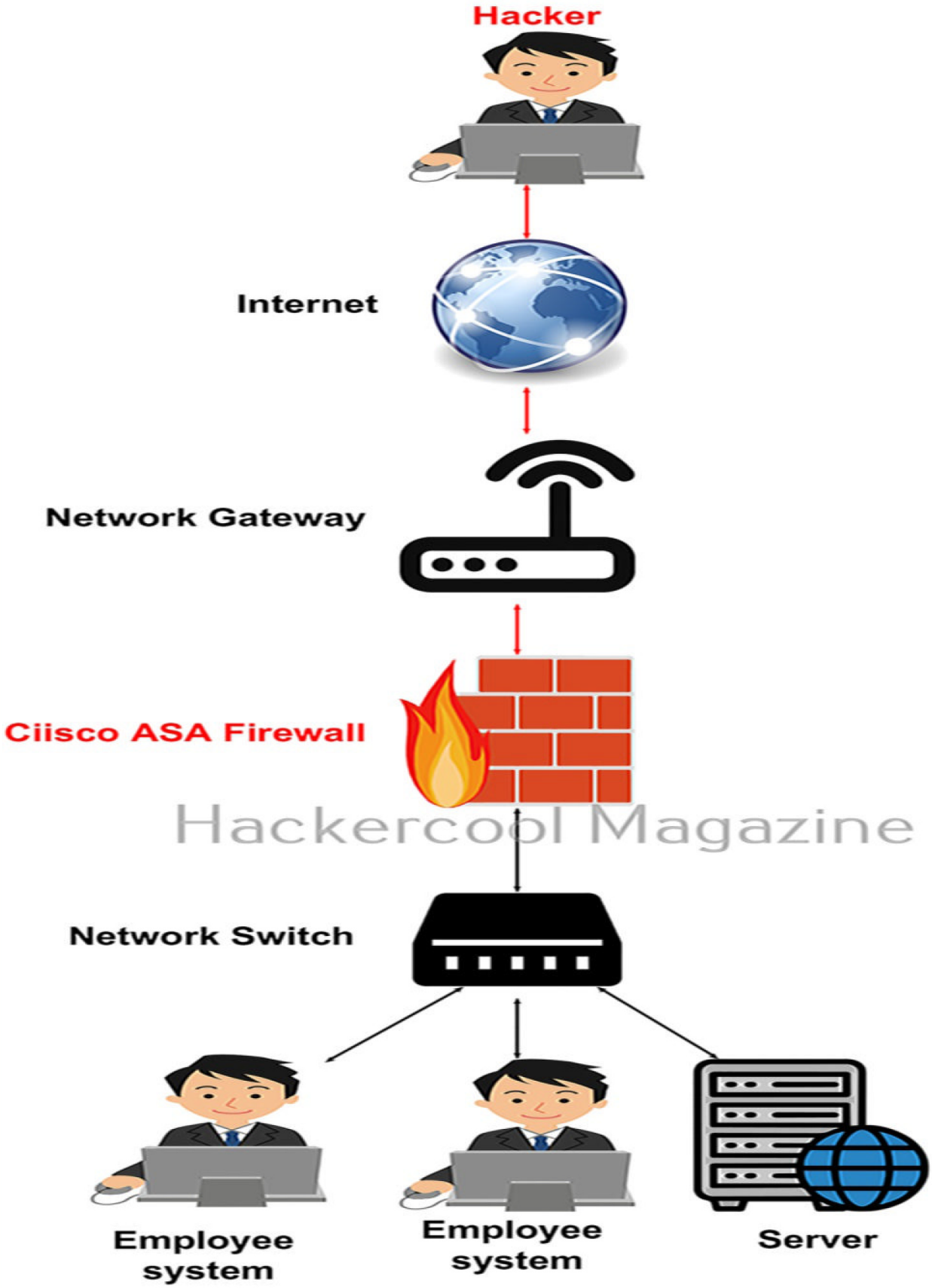


Fig: Exploitation scenario of CVE-2025-20333

How to manage this vulnerability?

Cisco has released emergency security updates to fix these vulnerabilities. So, users are advised to update their devices and software immediately given the critical nature of the vulnerability.

The versions safe from these vulnerabilities include Cisco ASA 9.16.4.85, 9.17.1.45, 9.18.4.47, 9.19.1.137, 9.20.3.7 and 9.22.1.1.3 and cisco FTD software 7.0.8.1, 7.2.9, 7.4.2.4 and 7.6.1.

Users should note that there is no work around for this vulnerability to mitigate its risk without applying security patches. Cisco also advised organizations to review their threat detection configurati -on on VPN services to detect authentication attempts.

If you find it complex to see if your version of Cisco firewall is vulnerable or not, Cisco provides a tool named Cisco software checker, that when run checks any cisco security advisories that impact a specific software release and fix them automatically.

"We also know that threat actors are going to use agentic AI for their own benefits. We are already seeing some of this. They are using it to launch new kinds of attacks."

–Vasu Jakkal (VP of Security, Microsoft)

ANONYMOUS ZONE

Tails 7.0 is released: What's new

The latest version of Tails operating system, the Tails 7.0 has been released recently. Let's see what's new in this latest version of Tails. To those newbies who have no idea what Tails is, it is The Amnesiac Incognito Live System. In simple terms, it is a privacy focused Linux distribution specifically designed to keep you anonymous and secure on internet.

Latest features to be excited about

One feature that can make you very excited about the latest version of Tails is its faster boot time. This improved boot time is thanks to the change of USB/ISO image compression algorithm to ztsd from xz. This will result in a 10-15 second faster boot on most machines.

Change of Base OS

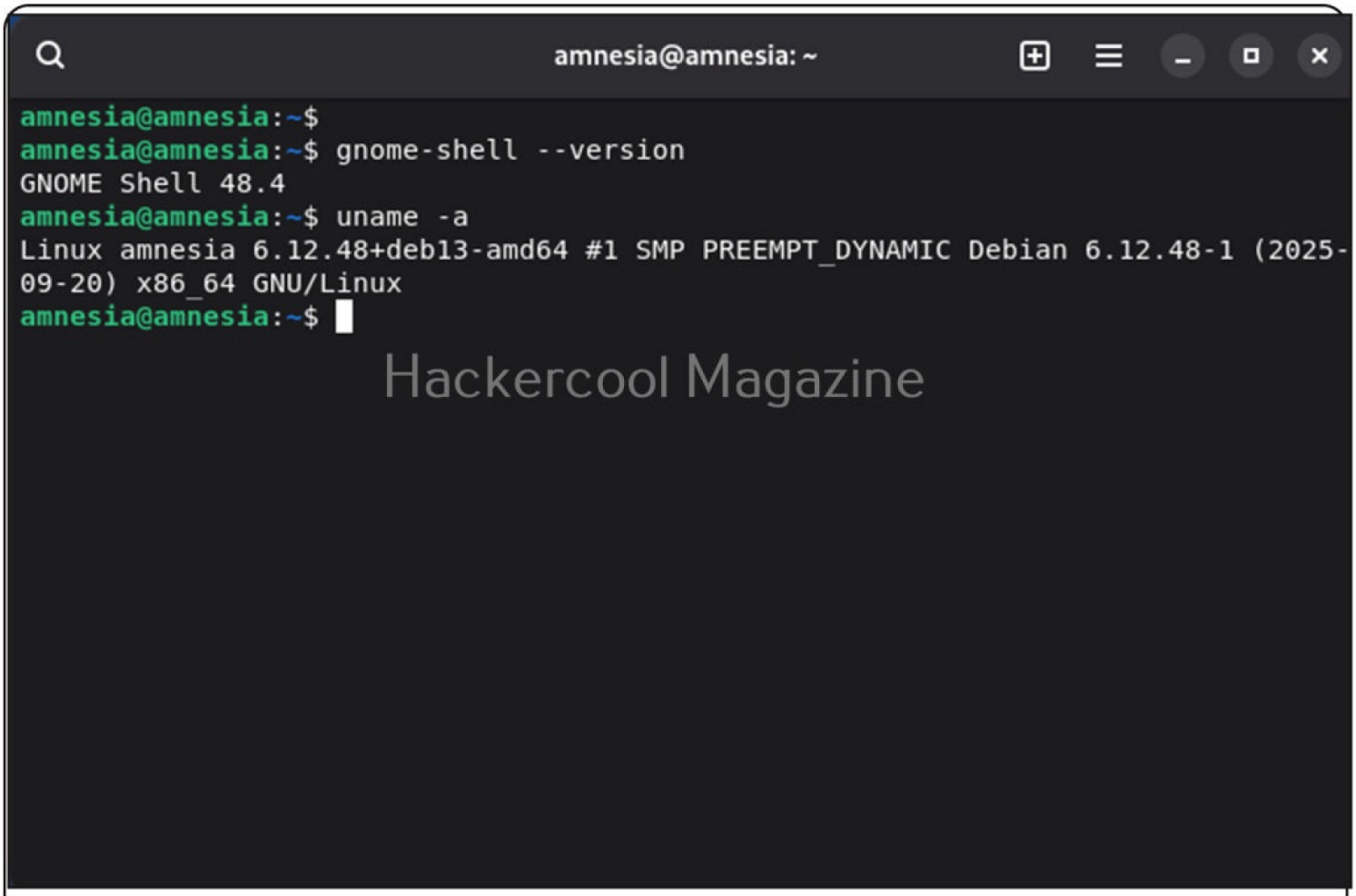
Tails 7.0 is based on Debian 13 "Trixie", the latest version of Debian which

means all the applications in the distro are updated. The Linux kernel is updated to version 6.12 and this gives support to newer hardware like graphics and Wi-Fi etc.

GNOME updated

Even the desktop environment has been updated to GNOME 48 which brings with it UI improvements and modern features. Most of the tools and applications have also been updated to newer versions. For example, Tor has been updated to version 14.5.7, Tor client has been updated to 0.4.8.17, Thunderbird to 128.14.0 ESR. Apart from these OnionShare, KeePassxc, Kleopatra, GIMP and Inkscape have all been updated to newer versions.

This version also brings lot of UX changes, which regular users might notice. The common terminal emulation has been changed to GNOME console from GNOME terminal. The default image viewer of Tails OS has been replaced with GNOME Loupe.

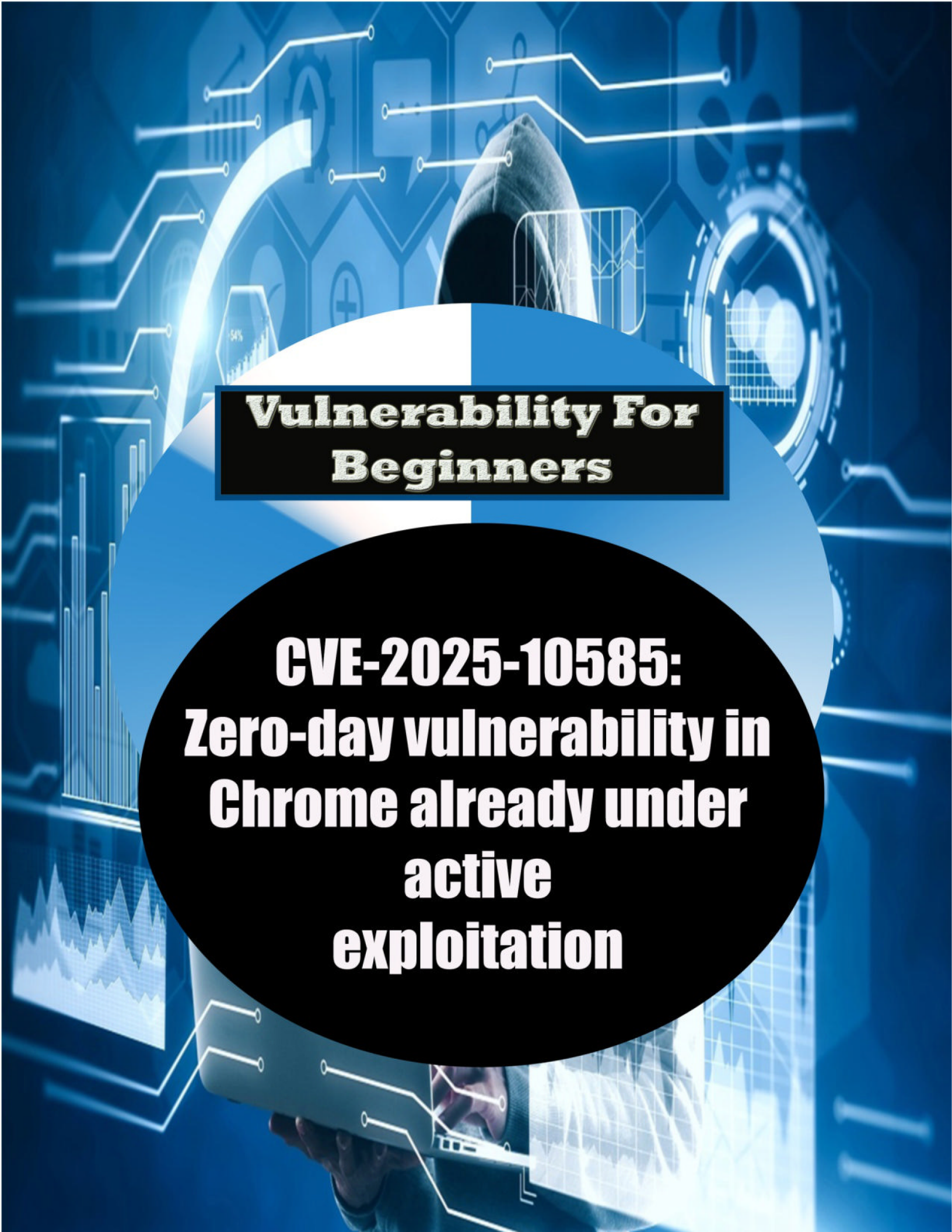


While some packages were updated, some packages have been removed. Also note that Tails now requires 3 GB of RAM instead of 2GB as minimum requirement.

Tails 7.0 is a key update compared to its previous versions and will definite -ly play a pivotal role in preserving your privacy.

"To me, the hack isn't just the end result. The hack is the process of learning and solving puzzles, figuring out things that weren't intended to be figured out."

– Chris Hadnagy


Vulnerability For Beginners
CVE-2025-10585: Zero-day vulnerability in Chrome already under active exploitation

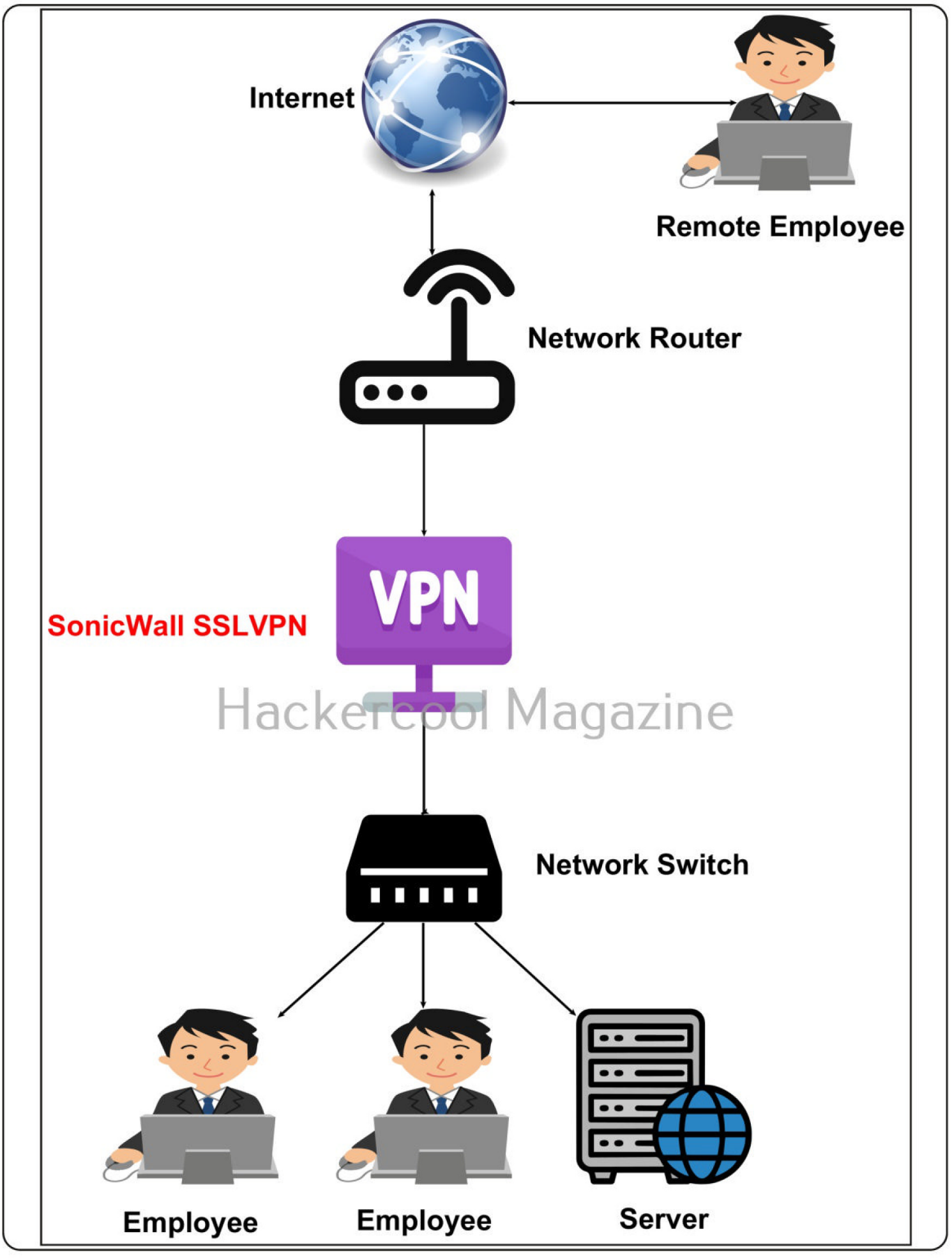
Researchers at Cybersecurity company Huntress have warned that Sonic-Wall SSLVPN devices are being compromised on a large scale around the world.

About the vulnerability

Threat actors are authenticating into multiple SonicWall devices using valid VPN credentials. The speed with which these logins are happening suggests that the attackers have valid credentials and definitely not brute forcing.

How the attackers got hold of so many valid accounts is the big question. A few days back SonicWall reported that there was a security incident which resulted in firewall configuration backup files stored in MySonicWall accounts getting exposed.

"Hackers are the immune system of the digital world." — Unknown


Internet
Remote Employee
Network Router
VPN
SonicWall SSLVPN
Hackercool Magazine
Network Switch
Employee
Employee
Server

This break affected all customers who use SonicWall cloud backup service. These configuration files contain important information like user, group, domain setting, DNS, log setting, certificate credentials.

However, cyber security company Huntress noted that there is no evidence to link this data breach to recent spike in logins. So, there may be even a zero-day vulnerability in SonicWall SSLVPN devices about which we know nothing yet.

Also, as the firewall configuration files contain highly sensitive data, they are encoded and not just that, credentials and secrets within the files are encrypted using the AES-256 hash algorithm. So, even if attackers successfully decode the configuration files, they will still need to decrypt credentials

This incident comes shortly after an increase in Akira ransomware targeting SonicWall SSLVPN devices for initial access by exploiting known vulnerability like CVE-2024-40766.

Impact

Millions of organizations around the world use SonicWall firewalls allowing SSLVPN remote access. The recent login actively started on October 4, 2025 and more than 100 SonicWall SSLVPN accounts across 16 customers have been breached. In some cases, attackers disconnected immediately after logging in.

However, in some other cases, hackers have conducted network scanning activity and tried to access local Windows accounts, compromising of which can have an impact on organizations.

How to manage your SonicWall devices?

No matter, how hackers are successfully logging into SonicWall firewalls, organizations using SonicWall SSLVPN devices are advised to reset their credentials immediately to prevent unauthorized access. They should also restrict WAN management and remote access wherever possible. Also revoke any

external API keys, enforce multi-factor authentication for all admin and rem-ote user accounts. They should all monitor logins for signs of any malicious activity.

Huntress proposed additional measures of security like disabling HTTP, H-TTPS, SSH and SSLVPN until all keys are rotated. External API keys, dyna-mic DNS and SMTP/FTP credentials should all be revoked. The reintroduct-ion of the service should be done in a staged manner to observe for any sus-picious activity.

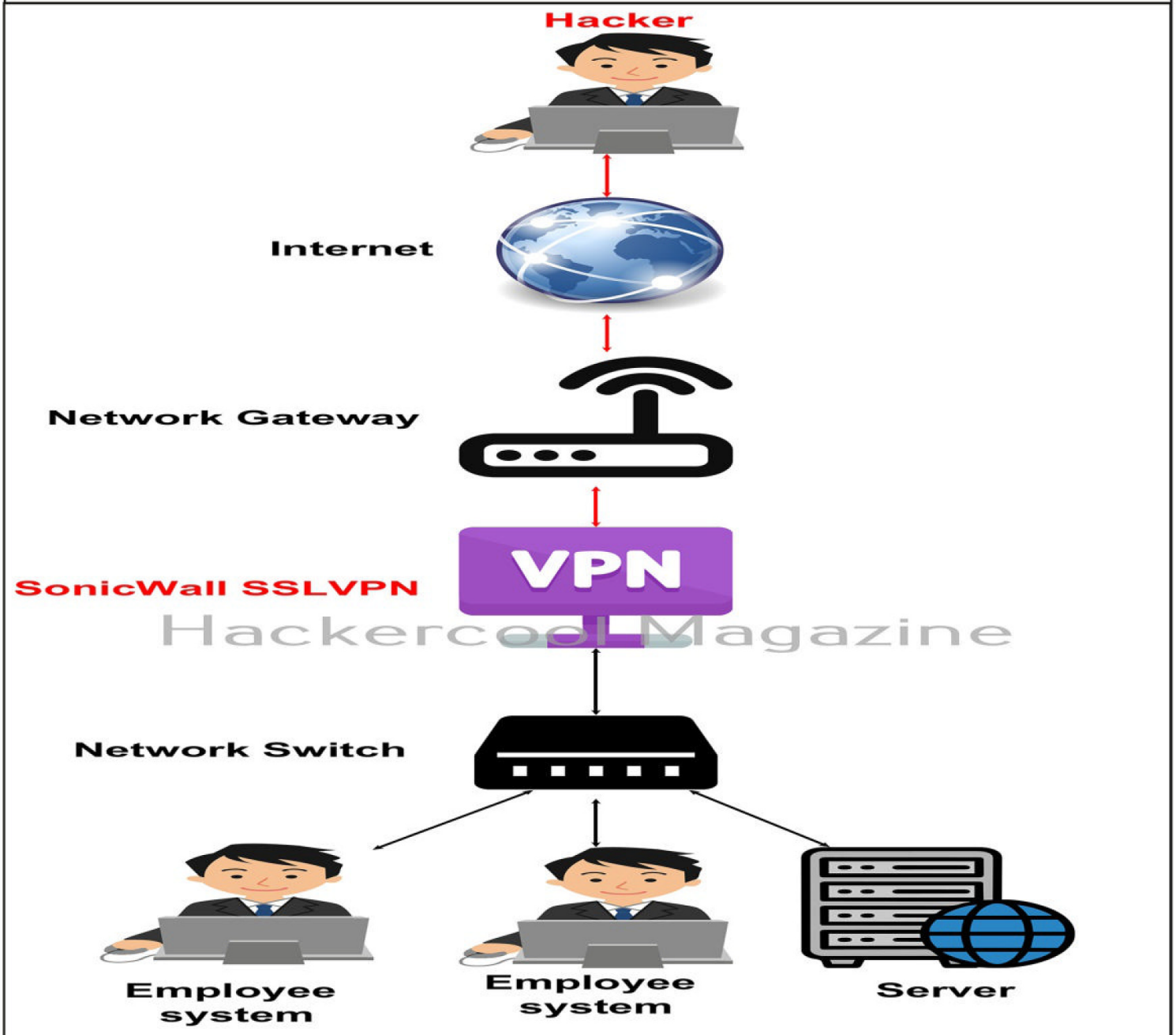


Fig: Exploitation scenario of recent breaches into SonicWall SSLVPN devices

MOBILE SECURITY

"Inside Klopatra: The stealthy Android Trojan draining bank accounts and taking complete control of the device"

An unknown malware strain is targeting thousands of Android users across Europe and stealing money from their bank accounts. Beware of this bankin-king Trojan.

KLOPATRA:
Beware of banking trojan that uses hidden VNC to control your Android phone

Hackercool Magazine

About the malware

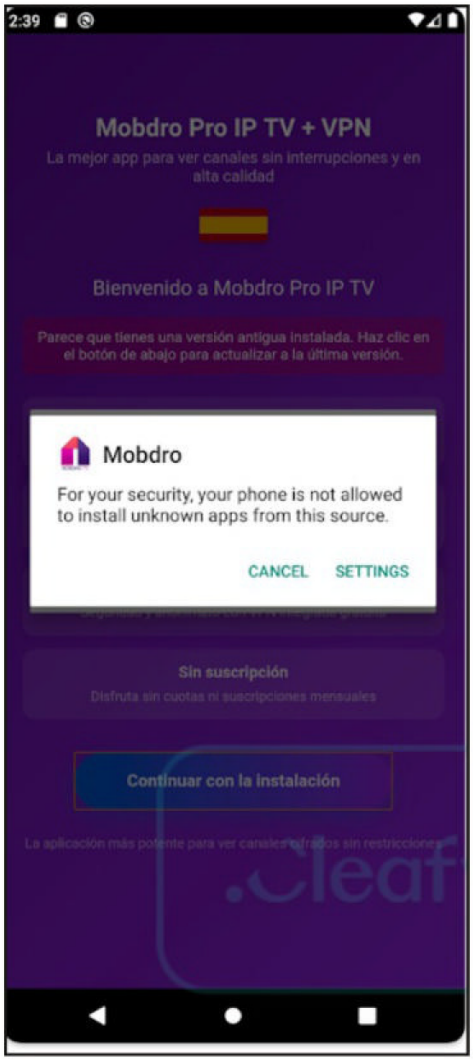
Klopatra was first discovered by Cleafy's Threat Intelligence team in late A-ugust 2025. This malware strain masquerades as a pirated TV and streamin-g app.

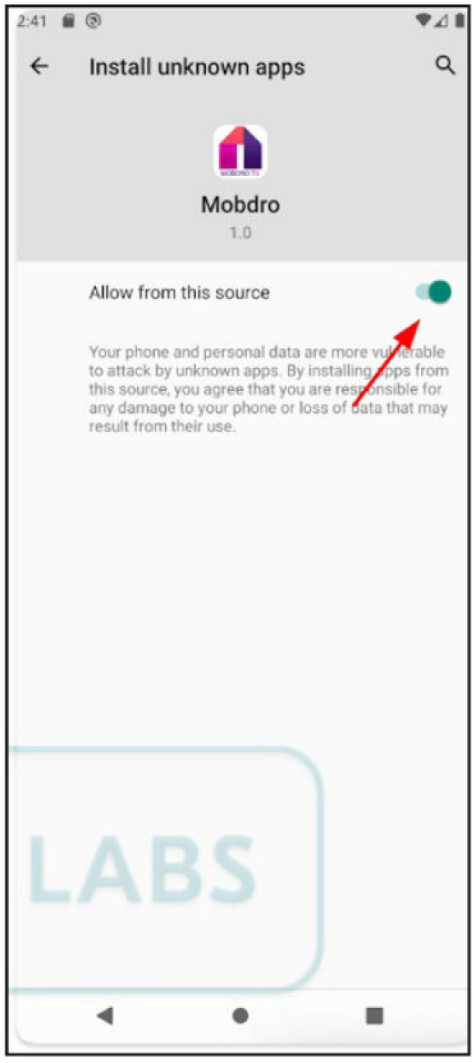
Method of infection

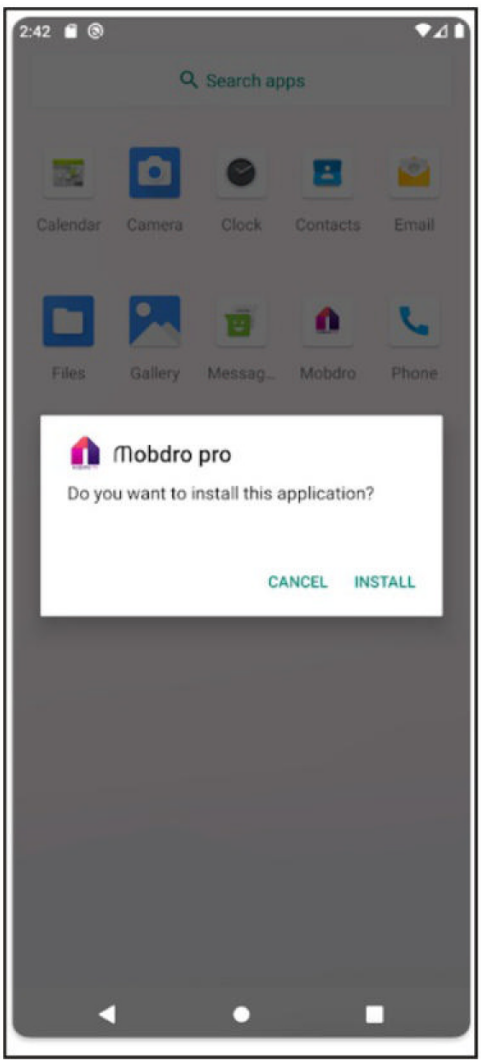
It specifically targets users searching for pirated TV streaming apps. This particular malware strain marquerades as "Mobdro Pro IP TV+VPN" an IPTV application.

2:38
Mobdro Pro IP TV + VPN
La mejor app para ver canales sin interrupciones y en alta calidad
Bienvenido a Mobdro Pro IP TV
Parece que tienes una versión antigua instalada. Haz clic en el botón de abajo para actualizar a la última versión.
+30.000 canales
Todos los canales españoles e internacionales sin interrupciones
Calidad HD/FHD
La mejor calidad de imagen y sonido sin errores
VPN integrada
Seguridad y anonimato con VPN integrada gratuita
Sin suscripción
Disfruta sin cuotas ni suscripciones mensuales
Continuar con la instalación
La aplicación más potente para ver canales cifrados sin restricciones

Since applications like these are not allowed on Google Play store, the targ-et users are tricked into downloading the applications from unknown source-s.







If the user falls for this and installs the application from external sources, th-e application convinces the user to grant critical permissions to the app on t-he device. The malware does this by presenting a simple user interface with a button as shown below. This button asks users to continue with the installa-tion. If you click on this button, it redirectd you to Android's system settings and instructs you to grant the permission.

POST installation mayhem

Once installed, Klopatra acts as both banking Trojan and a RAT. It takes full control of the target device and starts a hidden VNC (Virtual Network

Computing) server. Using this, attackers can take full control of the device a-nd control it in real-time. Hackers can see all the apps installed on your dev-ice, enter PINs and passwords and worst of all transfer money from your ba-nks without your knowledge. Klopatra can also grant itself additional permi-ssions to prevent itself from being deleted and even tries to uninstall Antivir-us apps installed on the device.

The highlight of this Android malware is the use of hidden VNC for remot-e controlling the infected device. Through VNC, remote attackers can even launch fake overlay login screens to spy on credentials. It can perform all th-ese activities without the target user realizing it. It can even exfiltrate clipboa-rd content and key strokes and can collect eve -n crypto currencies.

Impact

The Android malware is at present active in Spain and Italy and has infect-ed over 3000 devices. But this may just be a testing phase and malware may be spread to entire Europe especially targeting banking customers.

Cleafy's researchers say Klopatra has a high level of sophistication and eve-n uses Virbox, a commercial code protection program to prevent analysts fr-om studying its code.

How to manage this Android Trojan

All mobile users in Europe (at present) should be beware of this banking tr-ojan. To keep your Android device safe from attacks like this, stop installing apps from unknown sources and install only from Play Store. While installing any apps on your device, please check the permissions the app is requesting VERY CAREFULLY. If you see any app asking for permissions that it does-n't need, please don't give them. Many people just click on them.

Train your employees and users in the dangers of social engineering. Make sure you have an Antivirus app installed on your device.

CYBER SECURITY

The world's most sensitive computer code is vulnerable to attack. A new encryption method can help.

Qiang Tang
Associate Professor, Computer Science, University of Sydney

Moti Yung
Adjunct Research Professor, Computer Science, Columbia University

Yanan Li
PhD Candidate, School of Computer Science, University of Sydney

Nowadays data breaches aren't rare shocks – they're a weekly drumbeat. From leaked customer records to stolen source code, our digital lives keep spilling into the open.

Git services are especially vulnerable to cybersecurity threats. These are online hosting platforms that are widely used in the IT industry to collaboratively develop software, and are home to most of the world's computer code.

Just last week, hackers reportedly stole about 570 gigabytes of data from a git service called GitLab. The stolen data was associated with major companies such as IBM and Siemens, as well as United States government organisations.

In December 2022, hackers stole source code from IT company Okta which was stored in repositories on GitHub.

Cyberattackers can also quietly insert malicious code into existing projects without a developer's knowledge. These so-called "software supply-chain" attacks have turned development tools and update channels on git services into high-value targets.

"Cyberattackers can also quietly insert malicious code into existing projects without a developer's knowledge. These so-called "software supply-chain" attacks have turned development tools and update channels on git services into high-value targets."

As we explain in a new conference paper, our team has developed a new way to make git services more secure, with very little impact on performance.

The gold standard

We already know how to keep conversations private: secure messenger s-

(Cont'd On Next Page)

ervices such as Signal and WhatsApp use end-to-end encryption, which lock -s messages on your device and only unlocks them on the recipient's devic-e. This protects the data even if the se -rvice platform is hacked, which is wh -y it's considered the gold standard to protect data.

But git services, which are widely us -ed by major tech companies and star -tups, currently do-n't use end-to-end encryption. The s-ame is true for mo -st of the other too -ls we use to work together, such as s -hared documents.

Because git servi-ces allow a huge n -umber of collabor-ators to work on the same project at t-he same time, the software codes they host are constantly written and updat-ed at a very rapid rate. This makes using standard encryption impractica-l. To do so would take up too much bandwidth to transmit all of the data f -or even one word change, and make the services very inefficient.

But our new encryption method ove -rcomes this challenge.

Striking an important balance

The method we have developed use -s what's known as "character-level en -cryption". This means only edits to a software code stored on the git servic-e are treated as new data to be encry-pted – rather than the entire code.

Think of it as encrypting the tracked changes in a wor-d document, inste -ad of a new vers -ion every time.

This method str -ikes an important balance. It keeps the updated code private and secur-e while reducing the amount of co-mmunication bet-ween user and git services, as well as the amount of storage required.

Importantly, this new method is also compatible with existing git services, making it easy for people to adopt. It also doesn't interfere with other functi -ons of git servers, such as hosting, sa-ving bandwidth and indexing, so peo-ple can keep using these servers as th-

(Cont'd On Next Page)

"We already know how to keep conversations private: secure messenger services such as Signal and WhatsApp use end-to-end encryption, which locks messages on your device and only unlocks them on the recipient's device. This protects the data even if the service platform is hacked, which is why it's considered the gold standard to protect data."

-ese servers as they normally would – just with the added benefit of extra se -curity.

A broader end-to-end encrypted internet

This new tool is currently free and open-source for all users. It can be ins -talled easily like a patch when using git services, and will run in the backg- round as users access git services just like before.

But this is just the starting point for a broader shift towa -rds online collabo -ration that is secu- red by end-to-end encryption.

"The goal is not secrecy at all costs, but verifiable controls that respect both privacy and the rule of law."

Extending the same guarantees to sh -ared documents, spreadsheets and d- esign files is possible, but will require sustained research and investment.

One complication to ensure security is managing encryption keys or crede- ntials for users to decrypt encrypted d -ata. Fortunately, our previous researc -h shows us how to create a secure cl- oud storage system that will allow use -rs to safely store their credentials.

Just as importantly, we must balance security with compliance and account -ability. Universities, hospitals and go- vernment agencies are required to ret -ain and, in some cases, provide lawfu -l access to certain data. Meeting thes- e obligations, without weakening end- to-end encryption, pushes us to resear -ch new techniques.

The goal is not secrecy at all costs, b -ut verifiable controls that respect bot- h privacy and the rule of law.

We don't need a brand new internet to get there. We need pragmatic upgr -ades that fit the tools people already use – paired with clear, provable guar -antees.

Messaging prov- ed that end-to- end encryption c- an scale to billion -s. Code and cloud files are next, and with continued research and targeted investment, the rest of our everyday c -ollaboration can follow.

So before too long, you will hopeful- ly be able to work on a shared docu- ment with colleagues with the peace of mind that it, too, has gold standard security.

This article first appeared in The Conversation

DOWNLOADS

Cleverhans

https://github.com/cleverhans-lab/cleverhans

PowerShell Empire

https://github.com/BC-SECURITY/Empire

DeepFaceLab

https://github.com/iperov/DeepFaceLab

Resemble.ai

https://github.com/resemble-ai

Zeek

https://github.com/zeek/zeek

Suricata

https://github.com/OISF/suricata

OSQuery

https://github.com/osquery/osquery

Fleet

https://github.com/kolide/fleet

ElasticSearch

https://github.com/elastic/elasticsearch

OpenSearch

https://github.com/opensearch-project

DOWNLOADS

MISP

https://github.com/MISP/MISP

The HIVE + Cortex

https://github.com/TheHive-Project/Cortex

Kali Linux 2025.3

https://www.kali.org/get-kali/#kali-platforms

Tails 7.0

https://tails.net/install/index.en.html

USEFUL RESOURCES

Check whether your email is a part of any data breach

https://haveibeenpwned.com

Vulnera

https://github.com/hackercoolmagz/vulnera

Follow Hackercool Magazine for latest updates